المركز الديمقراطي العربي؛ برلين- ألمانيا

الجريمة المعلوماتية وأثرها على التنمية الاقتصادية



اشراف وتنسيق

د. مجدوب نوال

رئيس اللجنة العلمية

د. طالب محمد كريم

الجزء:02

كتاب جماعي

رقم التسجيل: VR.3373-6395.B

المركز الديمقراطي العربي

الجريمة المعلوماتية وأثرها على التنمية الاقتصادية



تأليف مجموعة من الباحثين

الجريمة المعلوماتية وأثرها على التنمية الاقتصادية

الجزء:02

إشراف و تنسيق:

د. مجدوب نوال



الناشر

المركز الديمقراطي العربي

للدراسات الاستراتيجية والسياسية والاقتصادية

ألمانيا/برلين

Democratic Arabic Center

Berlin / Germany

المركز الديمقراطي العربي

للدراسات الاستراتيجية والسياسية والاقتصادية ألمانيا/برلين

Berlin10315 Gensingerstr :112

Tel :0049-code Germany

54884375-030

91499898-030

86450098-030

البريد الإلكتروني

book@democraticac.de



رئيس المركز الديمقراطي العربي: أ.عمار شرعان

اسم الكتاب: الجريمة المعلوماتية و أثرها على التنمية الاقتصادية

الجزء:02

تأليف: مجموعة من الباحثين

إشراف والتنسيق: د. مجدوب نوال

رئيس اللجنة العلمية للكتاب: د. طالب محمد كريم

ضبط وتدقيق: د.سالم بن لباد

التصميم والإخراج: د. بدر الدين شعباني

رقم تسجيل الكتاب:VR.3373.6395.B

عدد الصفحات:

الطبعة الأولى

جويلية 2020 م

تأليف مجموعة من الباحثين

المحتويات

اللجنة العلمية للكتاب :

لجنة تحكيم الكتاب

رئيس لجنة التحكيم	د .طالب محمد كريم - المركز الجامعي مغنية

أعضاء لجنة التحكيم :

د. نعوم مراد المركز الجامعي مغنية	أ. د.حساني علي جامعة تيارت	أ.د. نداء مطشر صادق جامعة العراق
د. هاملي محمد المركز الجامعي مغنية	د. جزول صالح المركز الجامعي مغنية	د. بوزيدي إلياس المركز الجامعي مغنية
د. طالب محمد كريم المركز الجامعي	د. قارة سليمان محمد خليد	د. ميساوي حنان المركز الجامعي مغنية
د. المر سهام المركز الجامعي مغنية	د.الحاج علي بدر الدين المركز جامعي مغنية	د. شيماء الهواري - جامعة المغرب
د. بن عزوز فتيحة المركز الجامعي مغنية	د. بلعوشة شريف جامعة الإسكندرية	بوزيدي خالد المركز الجامعي مغنية
د. طالب دليلة جامعة تلمسان	د. مجدوب نوال المركز الجامعي مغنية	د. مجدوب خيرة جامعة تيارت
د. زياني عبد الحق جامعة تيارت	د. صورية بوربابة جامعة بشار	د. زروال معزوزة جامعة تلمسان
د. بلمختار سعاد المركز الجامعي مغنية	د. علاء مطر جامعة فلسطين	د. الحاسي مريم المركز الجامعي مغنية

تأليف مجموعة من الباحثين

د • عطار نسيمة المركز الجامعي مغنية	د• بن حمو فتح الدين المركز الجامعي مغنية	د• واسطي عبد النور المركز الجامعي مغنية
د• زينب عبد الله – جامعة النهرين	د• بن عودة صليحة المركز الجامعي مغنية	د• حسن مروان جامعة المغرب
د• حمادة خير جامعة العراق	د •عائشة الجميل جامعة الأسيوط	د•باعزيز أحمد المركز الجامعي مغنية
د• الأحسن محمد المركز الجامعي مغنية	د• تلعيش خالد جامعة خميس مليانة	د• حماس عمر المركز الجامعي مغنية
د• معاشو لخضر جامعة بشار	د• سويلم فضيلة جامعة سعيدة	د•دربال سهام المركز الجامعي مغنية



مقدمة

تأليف مجموعة من الباحثين

مقدمة الكتاب

لا يمكن إنكار المزايا التي قدمتها تكنولوجيا الإعلام و الاتصال في كافة مجالات الحياة ، إذ وبالقدر الذي ساهمت المعلوماتية في النهوض و التقدم و الرقي ، بقدر ما ساهمت في بروز نوع مستحدث من الإجرام و هو الإجرام المعلوماتي ، و الذي أخذ عدة تسميات و من ذلك الجريمة الإلكترونية ، جرائم الحاسوب ، جرائم تكنولوجيا الإعلام و الاتصال ، الجريمة الرقمية ،الجريمة السيبرانية ، جريمة الانترنيت، الجريمة الرقمية .

و بالتالي فالجريمة المعلوماتية تشكل نمط إجرامي مستحدث فرض نفسه على الواقع ، و تعرف على أنها كل سلوك إيجابي أو سلبي تقدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة من أجل تنفيذ فعل إجرامي.

و تأخذ الجريمة المعلوماتية عدة صور فقد يكون الغرض من ارتكابها التعدي على العرض والشرف، أو الأموال، أو المساس بنزاهة التجارة و أخلاقيات التسويق، أو الاعتداء على حقوق الملكية الفكرية ، بل و أكثر من كذلك فقد استهدفت الجريمة المعلوماتية قطاع الخدمات.

وانطلاقا من مضار الجريمة المعلوماتية فإن هذه الأخيرة تكيف من قبيل الجرائم الاقتصادية، باعتبار أنها تستنزف اقتصاديات الدول، و يترتب عنها نتائج تنعكس سلبا على التنمية الاقتصادية، مما حتم معه ضرورة تضافر الجهود الوطنية و الدولية.

ونظرا لذاتية الجريمة المعلوماتية فقد أخذ إجراءات المتابعة بدورها خصوصية، سواء من حيث التفتيش أو التحري، أو حتى العقوبة ولاسيما في ظل غموض الدليل الرقمي .

ولأنه يعتري تنظيم الجريمة المعلوماتية في التشريع الجزائري، و التشريعات المقارنة عدة إشكالات، كان لزاما الخوض في هذا الموضوع بشتى جوانبه و تفريعاته، من طرف ثلة من الباحثين والباحثات، اللذين أسهموا بجهودهم الجادة في إخراج هذا العمل المتواضع إلى النور.



المحور الثالث

المنازعات الماسة بالعقود الإدارية الإلكترونية

الإثبات في منازعات العقود الإدارية المبرمة بالطريقة الإلكترونية
- دراسة حالة الصفقات العمومية الإلكترونية -

Evidence in disputes of administrative contracts concluded via the electronic method- Study the case of electronic public deals -

د. **بوزيدي خالد** أستاذ محاضر "ب"
معهد الحقوق و العلوم السياسية
المركز الجامعي مغنية - الجزائر

مقدمة:

لقد شهد العالم طفرة تكنلوجية ورقمية كبيرة فرضت نفسها كوسيلة ودعامة فعالة لمختلف التعاملات المدنية والتجارية بل وحتى الإدارية، أدت إلى بروز وانتشار العقود الإلكترونية كعقود حديثة تبرم بوسائط رقمية ووسائل إلكترونية، وهو ما أحدث تطورا في المنظومة القانونية التي تأثرت هي الأخرى بهذا الشكل الجديد من العقود سواء في القانون المدني أو التجاري أو الإداري.

ففي المادة الإدارية وبفضل تبني العديد من الدول لنظام الإدارة الإلكترونية[1] وما صاحبه من تحول كبير في مفهوم النشاط الإداري، قد ساهم في تبني نظام العقود الإدارية الإلكترونية كأسلوب جديد لإدارة وتسيير المرافق العامة، وضمان الخدمة العمومية وكذا تحسين نوعيتها، بحيث سمحت تشريعات مقارنة عديدة بإمكانية إبرام هذا النوع من العقود بالطريقة الإلكترونية.

[1]- لم تظهر الإدارة الإلكترونية من فراغ، وإنما جاءت نتيجة تطور موضوعي يمتد إلى العقود الخمسة الأخيرة التي كانت من حصة القرن الماضي. أما مقدمات الإدارة الإلكترونية فتتمثل في انتشار استخدام نظم الحاسوب في أنشطة الأعمال منذ نهاية عقد الخمسينات والستينات حيث وجدت معظم المنظمات والمؤسسات العامة أن استخدامها للحاسوب سيعني الإسراع في إنجاز الأعمال واختصار للجهد والوقت والموارد. وكان من نتائج تطور استخدام نظم الحاسوب والاتصالات ظهور نظام التبادل الإلكتروني للبيانات لنقل البيانات والرسائل الهيكلية بين الأطراف المستفيدة...وهكذا نستطيع القول دون مبالغة أن ظهور نظم وشبكات التبادل الإلكتروني للبيانات كانت المهاد المادي والتقني لولادة تكنلوجيا الإدارة الإلكترونية. للمزيد حول الموضوع سعد غالب ياسين، الإدارة الإلكترونية، دار الياوزري العلمية للنشر والتوزيع، الأردن، 2010، ص 32

والمشرع الجزائري بدوره قد تأثر بهذا الوضع السائد بفضل الإصلاحات التي شهدتها منظومة الصفقات العمومية منذ سنة 1967[1]إلى غاية سنة 2015[2]، بحيث كرس نظام التعاقد الإلكتروني كأسلوب جديد للتعاقد الإداري لأول مرة من خلال المرسوم الرئاسي رقم 10-236[3]باعتماده نظام الاتصال وتبادل المعلومات بالطريقة الإلكترونية عبر البوابة الإلكترونية للصفقات العمومية، أعقبه صدور المرسوم الرئاسي رقم 15-247 الذي رسخ فكرة التعاقد الإداري الإلكتروني، تماشيا وصدور القرار الوزاري بتاريخ 17 نوفمبر 2013[4] الذي حدد محتوى البوابة الإلكترونية للصفقات العمومية وكيفيات تسييرها وكيفيات تبادل المعلومات بالطريقة الإلكترونية.

ونظرا لكون العقود الإدارية الإلكترونية تبرم بأساليب إلكترونية فإنها تتم بنوع جديد من الكتابة والتوقيع، بحيث يتم تبادل المعلومات بين المصالح المتعاقدة والمتعاملين الإقتصاديين عبر دعائم وقواعد بيانات إلكترونية توفرها البوابة الإلكترونية للصفقات العمومية، تسمح برقمنة الوثائق وتوقيعها بالطريقة الإلكترونية، وهو ما يثير إشكالية إثبات هذا النوع من العقود أمام القضاء الإداري في حالة وجود نزاع معروض أمامه.

ومما لا شك فيه أن هذا الموضوع يحتل أهمية قصوى بالنظر إلى حداثته وقلة الدراسات لا سيما فيما يتعلق بموضوع الإثبات في منازعات العقود الإدارية المبرمة بالطريقة الإلكترونية، بحيث تبرز ضرورة التعرض لطبيعة الإثبات في هذا النوع من العقود، للوقوف على الآثار المترتبة

[1]- تمثل سنة 1967 تاريخ صدور أول تنظيم للصفقات العمومية في الجزائر، بموجب الأمر رقم 67-90 ممضي في 17 يونيو 1967، منشور في الجريدة الرسمية عدد 52 مؤرخة في 27 يونيو 1967، ص 718، يتضمن قانون الصفقات العمومية

[2]- تمثل سنة 2015 تاريخ صدور آخر تنظيم للصفقات العمومية في الجزائر، بموجب المرسوم الرئاسي رقم 15-247 ممضي في 16 سبتمبر 2015، منشور في الجريدة الرسمية عدد 50 مؤرخة في 20 سبتمبر 2015، الصفحة 03، يتضمن تنظيم الصفقات العمومية وتفويضات المرفق العام

[3]- مرسوم رئاسي رقم 10-236 ممضي في 07 أكتوبر 2010، منشور في الجريدة الرسمية عدد 58 مؤرخة في 07 أكتوبر 2010، الصفحة 03، يتضمن تنظيم الصفقات العمومية

[4]- قرار مؤرخ في 17 نوفمبر 2013 يحدد محتوى البوابة الإلكترونية للصفقات العمومية وكيفيات تسييرها وكيفيات تبادل المعلومات بالطريقة الإلكترونية، منشور في الجريدة الرسمية عدد 21 مؤرخة في 09 أبريل 2014، الصفحة 27

عن ذلك لا سيما في يتعلق بحجية الإثبات وخصوصيته وانسجامه مع النظام القانوني الذي ينظم مادة العقود الإدارية بصفة عامة والصفقات العمومية بصفة خاصة.

بناء على ذلك فإن إشكالية هذه الدراسة تتمحور أساسا حول **مدى قابلية المحررات الإلكترونية للإعتداد بها كدليل للإثبات في العقود الإدارية المبرمة بالطريقة الإلكترونية؟**

هذا ما سنحاول الإجابة عليه في هذه الدراسة التي ارتأينا أن نقسمهما إلى قسمين:

أولا: مدى قابلية الكتابة الإلكترونية لإثبات العقد الإداري الإلكتروني

ثانيا: مدى قابلية التوقيع الإلكتروني لإثبات العقد الإداري الإلكتروني

أولا: مدى قابلية الكتابة الإلكترونية لإثبات العقد الإداري الإلكتروني

يتم إبرام العقود الإدارية الإلكترونية من خلال تبادل الوثائق والرسائل والمعلومات بين الإدارة العمومية والمتعاملين الإقتصاديين عبر دعائم وقواعد بيانات إلكترونية، على غرار دفاتر الشروط، والإعلانات عن المناقصات والدعوات للانتقاء الأولي ورسائل الإستشارات؛ العروض التقنية والمالية، بحيث يتم رقمنة تلك الوثائق وإرسالها وتوقيعها وحفظها بطريقة إلكترونية، ما يضفي على هذه المحررات الكتابية طابعا إلكترونيا يثور معه التساؤل حول مدى حجيتها وإمكانية الإعتداد بها كدليل إثبات في المنازعات المعروضة أمام القاضي الإداري.

1- مدى حجية الكتابة الإلكترونية كدليل للإثبات

لقد حاولت مختلف التشريعات الوطنية مسايرة التطور الناجم عن استخدام الوسائل الإلكترونية في مجال التعاقد، بإقرارها لنظام الكتابة الإلكترونية كآلية لتبادل الوثائق والبيانات عبر وسائط إلكترونية لا مكان فيها للتعامل بالمستندات والمحررات الورقية كما هو معمول به في إطار العقود الإدارية التقليدية. بحيث استحدثت نصوص قانونية في العديد من الدول خصت نظام الكتابة الإلكترونية بأحكام قواعد خاصة تتكيف مع طبيعتها وخصوصيتها، انطلاقا من مدلولها القانوني ووصولا إلى مدى حجيتها كدليل للإثبات.

ويمكن أن نلمس ذلك من خلال اطلاعنا على القانوني المدني الفرنسي[1] الذي اعترف صراحة بالكتابة الإلكترونية بإعطائه تعريفا لها على أنها **(تلك الكتابة التي تشمل كل تدوين**

---

[1]- تنص المادة 1316 من القانون المدني الفرنسي على ما يلي:

(La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels

لحروف أو المعاملات أو الأرقام، أو أية إشارات أو رموز ذات معنى واضح، أيا كانت الدعامة التي تستخدم لإنشائها أو الوسيط الذي تنتقل عبره).

ويبدو من خلال هذا التعريف بأن المشرع الفرنسي قد أعطى مفهوما واسعا للكتابة الإلكترونية التي لم يحصر نطاق انتقالها في وسيلة أو طريقة معينة، لتشمل سلسلة العلامات والرموز التي يجري إنشائها وتداولها على مختلف الوسائط الإلكترونية. ولعل تبني المشرع الفرنسي لهذا التعريف يعود بالدرجة الأولى إلى تأثره بما جاء في قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية[1] الذي أورد تعريفا شاملا وموسعاللكتابة الإلكترونية، بحيث عرفها في **المادة 02** فقرة أبأنها **(تلك المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل الكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الإلكترونية، أو البريد الإلكتروني، أو البرق أو التلكس، أو النسخ البرقي).**

وقد قد أورد المشرع الجزائري مدلولا مشابها للكتابة الإلكترونية لذلك الذي أورده المشرع الفرنسي وقانون الأونيسترال النموذجي بشأن التجارة الإلكترونية، حينما عرف الكتابة الإلكتروني في **المادة 323 مكرر** من القانون المدني الجزائري[2] بقولها **(ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها).**ويبدو من خلال هذا التعريف أن المشرع الجزائري قد أعطى كذلك مفهوما عاما للكتابة الإلكترونية مشابها لسابقيه، ليشمل فيما يشمل جميع الوثائق والبيانات والمعلومات التي يتم إنشاؤها أو تداولها أو حفظها أو رقمنتها بصرف النظر عن الدعامة أو الوسيلة الإلكترونية المستعملة في ذلك.

---

que soient leur support et leurs modalités de transmission). Article 1316, Modifié par Loi n°2000-230 du 13 mars 2000 - art. 1 JORF 14 mars 2000

[1]- قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، تاريخ الإعتماد 12 يونيو 1996، منشور على الموقع الإلكتروني التالي، تاريخ الاطلاع 04 إبريل 2020:

https://uncitral.un.org/ar/texts/ecommerce/modellaw/electronic_commerce

[2]- الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني المعدل والمتمم، منشور في الجريدة الرسمية العدد 78 المؤرخة في 30 سبتمبر 1975

وجدير بالإشارة هنا إلى أنه إذا كان العقد الإداري يخضع في إبرامه لنظام قانوني متميز عن تلك القواعد التي تحكم وتنظم عملية إبرام العقود الخاصة[1]، فإنه لا يعني البتة وجود اختلاف في مفهوم الكتابة الإلكترونية في القانونين العام والخاص، بحيث أن المعنى المشار إليه في النصوص القانونية المذكورة أعلاه ينطبق على العقود الخاصة الإلكترونية كما ينطبق كذلك على العقود الإدارية الإلكترونية، من منطلق أن القضاء الإداري ممثلا في مجلس الدولة الفرنسي غالبا ما يطبق في بعض القضايا في موضوع العقود الإدارية نصوص القانون المدني، على غرار القواعد المقررة في القانون المدني بخصوص القوة القاهرة والحادث المفاجئ، ما دامت تلك القواعد لا تتعارض مع طبيعة وخصوصية الروابط القانونية الناشئة في مجال القانون العام[2].

ويمكن أن نلمس ذلك من خلال موقف العديد من التشريعات الوطنية التي ساوت بين طبيعة الكتابة التقليدية والكتابة الإلكترونية في مجال المعاملات المدنية والإدارية من حيث حجيتها، بحيث اعترف المشرع الفرنسي في المادة 1316-1 من القانون المدني الفرنسي بحجية المحررات والمستندات الإلكترونية، وأعطى لها حجية قانونية كتلك التي تحوزها المحررات والمستندات العادية[3].

---

[1]- بحيث يخضع العقد الإداري لقواعد القانون العام، بينما تخضع العقود الخاصة لقواعد القانون الخاص لا سيما القانون المدني، على أنه لا يمكن أن يعتبر عقدا إداريا يخضع لأحكام القانون العام إلا إذا توافر فيها شرطين أساسيين وهما: أن يكون أحد طرفي العقد شخصا من أشخاص القانون العام، وأن تأخذ الإدارة في العقد بأساليب القانون العام إما بأن يتضمن العقد شروط استثنائية غير مألوفة و/أو يشترك المتعاقد مع الإدارة في تسيير وإدارة مرفق عام. للمزيد حول هذا الموضوع راجع زكريا المصري، العقود الإدارية ما بين الإلزام القانوني والواقع العملي دراسة مقارنة محلية ودولية، دار الفكر والقانون للنشر والتوزيع، الطبعة الأولى، مصر، 2014، ص 16 وما بعدها

[2]- أنظر حكم مجلس الدولة الفرنسي الصادر بتاريخ 17 ديسمبر في قضية Grands moulins de Corbeil حيث أشار مجلس الدولة الفرنسي صراحة إلى المادة 1116 من القانون المدني المتعلق بالغش. وحكمه الصادر كذلك بتاريخ 09 فبراير 1951 في قضية Ste Bornhauser حيث أشار مجلس الدولة الفرنسي إلى المادة 1917 من القانون المدني الفرنسي. راجع في هذا الخصوص سليمان محمد الطماوي، الأسس العامة للعقود الإدارية دراسة مقارنة، دار الفكر العربي، مصر، 2012، ص 22

[3]- تنص المادة 1316-1 من القانون المدني الفرنسي على ما يلي:

(L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier). Créé par Loi n°2000-230 du 13 mars 2000 - art. 1 JORF 14 mars 2000, Abrogé par Ordonnance n°2016-131 du 10 février 2016 - art. 3

وقد سار المشرع الجزائري على خطى نظيره الفرنسي، بإعطاءه للكتابة الإلكترونية نفس الحجية الممنوحة للكتابة على الورق في الإثبات، بموجب المادة 323 مكررا1 من القانون المدني الجزائري التي نصت على أنه (يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق...).

إلا أن ما يأخذ على المشرع الجزائري هو عدم تبيانه درجة حجية المحررات الإلكترونية في المعاملات الإدارية على غرار المعاملات المدنية درءا لأي تأويل، طالما أنه قد أقر بإمكانية إبرام العقود الإدارية بالطريقة الإلكترونية بموجب المرسوم الرئاسي رقم 10-236 المتضمن تنظيم الصفقات العمومية[1]، ثم بموجب المرسوم الرئاسي رقم 15-274 المتضمن تنظيم الصفقات العمومية وتفويضات المرفق العام[2]، فلا نكاد نلمس نصا قانونيا صريحا يشير إلى حجية المحررات الإلكترونية التي يجري تبادلها بين المصالح المتعاقدة والمتعاملين الاقتصاديين في البوابة الإلكترونية للصفقات العمومية، على غرار القرار المؤرخ في 17 نوفمبر 2013 الذي يحدد محتوى البوابة الإلكترونية للصفقات العمومية وكيفيات تسييرها وكيفيات تبادل المعلومات بالطريقة الإلكترونية، وإن كان نص المادة 12 منه تشير ضمنا حسب رأي الباحث إلى قوة حجية العروض الإلكترونية من حيث الإثبات، بنصها على إمكانية إيداع نسخ بديلة من العروض على حامل مادي ورقي، عندما يرد المتعهدون أو المترشحون للصفقات العمومية على إعلانات المنافسة بالطريقة الإلكترونية، على أن لا تفتح النسخة البديلة إلا إذا كان العرض المرسل بالطريقة الإلكترونية يحمل فيروسا، أو لم يصل في الآجال القانونية، أو لم يتمكن من فتحه. وعلى العموم فإنه يمكن تفسير هذا الموقف من المشرع الجزائري إلى كون أن هذا النمط المستحدث من التعاملات الإلكترونية في مجال الصفقات العمومية لم يتجاوز مرحلة التجربة خلال هذه الفترة[3].

وذلك بخلاف المشرع الفرنسي الذي كان أكثر وضوحا، حينما منح للمحررات الإلكترونية حجية قانونية كالمحررات الورقية في مجال العقود الإدارية، وذلك بموجب المادة 56 فقرة 03 قانون الصفقات العمومية الفرنسي الصادر سنة 2000، المعدل بالمرسوم رقم 15-

---

[1]- راجع المادتين 173 و174 من المرسوم الرئاسي رقم 10-236

[2]- راجع المواد 203 و204 و205 و206 من المرسوم الرئاسي رقم 15-247

[3]- راجع في هذا الخصوص بوزيدي خالد، الإتصال وتبادل المعلومات بالطريقة الإلكترونية كإجراء جديد لتعزيز مبادئ الشفافية والمساواة في مجال الصفقات العمومية، مجلة حقوق الإنسان والحريات العامة، العدد السادس، جوان 2018، مستغانم الجزائر، ص 278 وما بعدها

2004التي نصت على أن (كل النصوص للمرسوم الحالي والخاصة بالكتابة، يمكن تحويلها إلى كتابة على وسيط إلكتروني)، وهو ذات الموقف الذي رسخه مجلس الدولة الفرنسي في العديد من قراراته[1] التي أكدت على شرعية المحررات الإلكترونية، وجواز استعمالها في الإثبات مثلها مثل المحررات الكتابية[2].

2- شروط الإعتداد بالكتابة الإلكترونية كدليل إثبات

إذا كانت النصوص القانونية قد ساوت بين الحجية القانونية للكتابة الإلكترونية والكتابة الورقية العادية كدليل للإثبات، فإنها قد ربطت في مقابل ذلك درجة قوة حجيتها بمدى توافر مجموعة من الشروط حتى يتسنى الاعتداد بها كدليل إثبات، بحيث يشترط أن تكون الكتابة الإلكترونية قابلة للقراءة، وأن تكون قابلة للحفظ والاستمرار، وأن تكون غير قابلة للتعديل.

أ- قابلية الكتابة الإلكترونية للقراءة

يشترط في الكتابة الإلكترونية حتى تكون قابلة للإعتداد بها كدليل إثبات في منازعات العقود الإدارية المبرمة بالطريقة الإلكترونية أن تكون قابلة للقراءة، وذلك بأن تكون مدونة بحروف أو رموز مفهومة، وهو ما حرص المشرع الجزائري على تأكيده من خلال المادة 323 مكرر 1 من القانون المدني التي نصت على أن (الإثبات بالكتابة ينتج من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم...)، وذلك على غرار ما ذهب إليه المشرع الفرنسي في نص المادة 1316 من القانون المدني الفرنسي التي سبق الإشارة إليها

1- حيث أكد مجلس الدولة الفرنسي في نظره لإحدى الطعون الإنتخابات على وصول الطعن الإنتخابي في الميعاد المقرر (خمسة أيام بعد يوم الإنتخابات) عن طريق الرسائل الإلكترونية، وما يثبت رسمية هذا المحرر الإلكتروني الرسالة الموجهة من الطاعن إلى المحكمة الإدارية، والتي بموجبها يتحقق من شخصية الطاعن، ولقد اعتبر مجلس الدولة الفرنسي هذا الخطاب المرسل عن طريق الوسيط الإلكتروني، بمثابة دليل كتابي كامل له حجية المحررات العرفية في الإثبات مثله مثل المحررات الكتابية التقليدية الأخرى، وذلك ما استوفى شروط الصحة المنصوص عليها في المواد 1316-1316-4 من القانون المدني الفرنسي. أشار إلى ذلك علي جبير عبيد الجنابي، الطبيعة القانونية للعقد الإداري الإلكتروني، مذكرة ماجستير في القانون العام، جامعة الشرق الأوسط، كلية الحقوق، الأردن، 2017، ص 115-116

2- راجع في هذا الخصوص قيدار عبد القادر صالح، إبرام العقد الإلكتروني وإثباته، مجلة الرافدين للحقوق، المجلد 10، العدد 37، السنة 2008، ص 172 و173

أعلاه[1].وهو ما توصل إليه مجلس الدولة الفرنسي سنة 1998 في تقريره المتعلق بالإثبات بالمحررات الإلكترونية الذي أكد على أن (المحررات الإلكترونية يجب أن تكون بشكل واضح ومفهوم للآخرين، خاصة القاضي لتكون دليلا للإثبات)[2].

ومما لا شك فيه أنه وفي حالة العقود الإدارية الإلكترونية فإنه يجري تدوينها على وسائط إلكترونية عن طريق حاسوب آلي، ما قد يجعلها غير مقروءة لدى الإنسان بشكل مباشر، ومن ثمة يتوجب حتى تستوفي الكتابة الإلكترونية لشرط القابلية للقراءة أن تكون هذه الحواسيب الآلية مدعمة ببرامج ودعائم إلكترونية لها القدرة على ترجمة لغة الآلة إلى لغة مقروءة لدى الإنسان[3].

غير أنه وبالنظر إلى السلطة التقديرية التي يتمتع بها القاضي الإداري فإنه له من الصلاحيات ما يمكنه من التعامل مع المحررات الإلكترونية التي قد تفتقد لشرط القابلية للقراءة والفهم، عن طريق إستعانته بأهل الخبرة في هذا المجال، في حالة ما إذا كانت هذه المحررات الإلكترونية غير مفهومة وواضحة، بأن كانت مشفرة أو محمية بنظام تقني خاص[4].

ب- قابلية الكتابة الإلكترونية للحفظ والإستمرار

فحتى يكون للكتابة الإلكترونية حجية قانونية كمثيلتها الورقية في منازعات العقود الإدارية المبرمة بالطريقة الإلكترونية، لا بد أن تكون البيانات والمعلومات الواردة فيها قابلة للحفظ والتخزين بحيث يمكن استرجاعها متى كان ذلك لازما حتى يتسنى لأطراف العقد أو القاضي مراجعتها والاطلاع عليها في حالة وجود نزاع قائم بين أطرافه حول بنود العقد الإداري أو كيفية تنفيذه.

وهو ما أكدته المادة 323 مكرر 1 من القانون المدني الجزائري التي نصت على اعتبار الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق بشرط (أن تكون معدة

---

[1]- راجع بخصوص المادة 1316 من القانون المدني الفرنسي ما سبق الإشارة إليه في هذه الدراسة في الصفحة 03 و04

[2]- أشار إليه فيصل عبد الحافظ الشوابكة، النظام القانوني للعقد الإداري الإلكتروني، مجلة الجامعة الإسلامية للدراسات الإقتصادية والإدارية، المجلد الحادي والعشرون، العدد الثاني، يونيو 2013، ص 353

[3]- صفاء فتوح جمعة، مسؤولية الموظف العام في إطار تطبيق نظام الإدارة الإلكترونية، دار الفكر والقانون للنشر والتوزيع، الطبعة الأولى، مصر، 2016، ص 104

[4]- فيصل عبد الحافظ الشوابكة، المرجع السابق، ص 353

ومحفوظة في ظروف تضمن سلامتها)، وذلك على غرار ما ذهب إليه المشرع الفرنسي في المادة 1316-1 من القانون المدني الفرنسي[1].

ويبدو أن المشرع الجزائري قد أعطى لهذا الشرط درجة بالغة من الأهمية في مجال العقود الإدارية المبرمة بالطريقة الإلكترونية، حينما نص على إلزامية أن يتضمن تسيير البوابة الإلكترونية للصفقات العمومية صيانة البوابة، لا سيما بضمان مستوى أمن مناسب ضد التهديدات الإلكترونية، إضافة إلى ديمومة واستمرارية وإمكانية الدخول للخدمات المقدمة من طرف البوابة[2].

تماشيا مع ذلك وحتى تكون الكتابة الإلكترونية في مجال العقود الإدارية المبرمة بالطريقة الإلكترونية معدة ومحفوظة في ظروف تضمن سلامتها، فقد أوجب المشرع الجزائري ضرورة أن يصمم نظام المعلوماتية للصفقات العمومية في إطار احترام مبدأ سلامة الوثائق المتبادلة بالطريقة الإلكترونية، على النحو الذي تضمن صيغ وأشكال رقمنة الوثائق المكتوبة عدم المساس بسلامته، في ظل احترام مبدأ سرية الوثائق المتبادلة بالطريقة الإلكترونية عن طريق نظام ترميز الوثائق مع احترام الأحكام التشريعية والتنظيمية المعمول بها[3].

وقصد مواجهة أي خطر محتمل قد يهدد سلامة هذه المحررات الإلكترونية، فقد أوجب المشرع الجزائري على المصلحة المتعاقدة التي تكتشف فيروسا في الوثائق المتعلق بالملف الإداري أو العرض أن تطلب من المتعهد أو المترشح القيام بإرسال آخر، وفي حالة ما إذا لم يتم إرسال النسخة البديلة أو تم إرسالها وكانت تحتوي على فيروس، تجري المصلحة المتعاقدة محاولة لإصلاح العرض أو النسخة البديلة وتواصل تقييم العروض إذا نجح الإصلاح.

[1]- تنص المادة 1316-1 من القانون المدني الفرنسي على ما يلي:

(L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité)

[2]- المادة 06 من القرار الوزاري المؤرخ في 17 نوفمبر 2013 المتضمن تحديد محتوى البوابة الإلكترونية للصفقات العمومية وكيفيات تسييرها وكيفيات تبادل المعلومات بالطريقة الإلكترونية

[3]- المادة 07 من القرار الوزاري المؤرخ في 17 نوفمبر 2013 المتضمن تحديد محتوى البوابة الإلكترونية للصفقات العمومية وكيفيات تسييرها وكيفيات تبادل المعلومات بالطريقة الإلكترونية

علما بأن المشرع الجزائري قد اعتبر الملفات التي تحتوي على فيروس والتي كانت محل محاولة إصلاح فاشلة، ملغاة أو غير كاملة. ويتم الاحتفاظ بأثر الفيروس وإبلاغ المتعامل الاقتصادي المعني، بذلك[1].

ت- عدم قابلية الكتابة الإلكترونية للتعديل

إن قدرة المستند الإلكتروني للإعتداد به كدليل إثبات تتقرر بمدى سلامته من أي عيب قد يؤثر في شكله الخارجي، ولا يتحقق ذلك إلا إذا كان المستند الإلكتروني غير قابل للتعديل أو التغيير من حذف أو محو أو حشو[2]، وهو ما يستوجب أن تتوفر المنصات الإلكترونية التي يجري خلالها حفظ وتبادل الوثائق والمستندات على أنظمة وبرامج معلوماتية يجري إعدادها وتصميمها من أجل أن يجعل هذه المحررات الإلكترونية قابلة للقراءة والفهم دون المساس بمضمونها، بتعطيل خاصية التعديل أو الإتلاف أو المحو أو الحشو لدى أطراف العقد الإداري.

وفي هذا السياق يشدد الفقه[3] على ضرورة قبول القاضي بصفة عامة والقاضي الإداري بصفة خاصة للمحررات الإلكترونية كدليل كامل متى تم تأمين بياناتها، وإلا أدى ذلك إلى إضعاف الثقة في المحررات الإلكترونية، وهو ما يستوجب حسبهم تدخل المشرع بالنص صراحة على اعتماد التكلوجيا المعتمدة في تأمين بيانات المحررات الإلكترونية بما يجعلها تستوفي شرط عدم القابلية للتعديل، دون الحاجة إلى ترك مسألة تقدير مدى توافر هذا الشرط للقاضي. وهو الإتجاه الذي يبدو بأن المشرع الجزائري يسايره حيث نص في القرار الوزاري المؤرخ في 17 نوفمبر 2013 على ضرورة حماية الوثائق المتبادلة عن طريق نظام ترميز الوثائق بما يضمن سلاماتها، على النحو الذي يستحيل من خلاله تعديل الوثيقة الإلكترونية أو إتلافها أو محوها[4].

ثانيا: مدى قابلية التوقيع الإلكتروني لإثبات العقد الإداري الإلكتروني

يعتبر التوقيع شرطا أساسيا لاعتماد العقد الإداري ودخوله حيز التنفيذ، وعلى هذا النحور فإن العقد الإداري الإلكتروني المبرم بالطريقة الإلكترونية لا يكون نهائيا إلا إذا ما تم اعتماده

---

[1]- راجع المادة 14 من القرار الوزاري المؤرخ في 17 نوفمبر 2013 المتضمن تحديد محتوى البوابة الإلكترونية للصفقات العمومية وكيفيات تسييرها وكيفيات تبادل المعلومات بالطريقة الإلكترونية

[2]- عصمت عبد المجيد بكر، دور التقنيات العلمية في تطور العقد، دار الكتب العلمية، لبنان، 2015، ص 337

[3]- راجع في هذا الخصوص صفاء فتوح جمعة، مسؤولية الموظف العام في إطار تطبيق الإدارة الإلكترونية، المرجع السابق، ص 108

[4]- أنظر المادة 07 من القرار الوزاري المؤرخ في 17 نوفمبر 2013 المتضمن تحديد محتوى البوابة الإلكترونية للصفقات العمومية وكيفيات تسييرها وكيفيات تبادل المعلومات بالطريقة الإلكترونية

من قبل السلطة المختصة عن طريق التوقيع الإلكتروني[1]، الذي يمكن التعامل به في هذا المجال إما من خلال التوقيع الرقمي أو الكودي أو البيومتري أو بالقلم الإلكتروني، وهو بهذه الشاكلة يعد عنصرا مهما من عناصر الإثبات في مجال منازعات العقود الإدارية المبرمة بالطريقة الإلكترونية، ما يستوجب منا البحث في مدى حجة التوقيع الإلكتروني كدليل للإثبات في هذا المجال، من خلال التعرض إلى مفهوم التوقيع الإلكتروني وشروطه لإثبات العقد الإداري الإلكتروني.

1- تعريف التوقيع الإلكتروني

بالنظر إلى حداثة مصطلح التوقيع الإلكتروني والأهمية التي يكتسبها في التعاملات الإلكترونية بما في ذلك العقود الإدارية الإلكترونية باعتباره شرطا لصحتها وسلامتها من الناحية القانونية، فقد قامت جل التشريعات بإعطاء تعريف للتوقيع الإلكتروني على غرار المساهمات الكثيرة التي قدمها الفقه في هذا المجال.

ومن بين التعريفات المقارنة يمكن أن نشير إلى التعريف الذي ساقه المشرع الفرنسي للتوقيع الإلكتروني بموجب المادة 1316-4من القانون المدني التي نصت على أن التوقيع الإلكتروني هو ذلك (التوقيع الذي ينتج عن استخدام وسيلة مقبولة موثوق بها تضمن اتصال التوقيع بالعمل أو المستند المرتبط به لإتمام التصرف القانوني، بما يعبر عن رضا الأطراف بالالتزامات المترتبة عن هذا التصرف، وتؤكد شخصية صاحبه وصحة الواقعة المنسوبة إليه حتى يثبت عكس ذلك)[2].ويبدو من خلال هذا التعريف أن المشرع الفرنسي لم يتأثر بالتعريف الذي أوردته لجنة

---

[1]- المادة 04 من المرسوم الرئاسي رقم 15-247

راجع كذلك بخصوص مرحلة الإعتماد والتوقيع الإلكتروني بين طرفي العقد الإداري، إيراين نوال، النظام القانوني للعقود الإدارية الإلكترونية دراسة حالة الصفقات العمومية الإلكترونية، مداخلة ملقاة خلال فعاليات المؤتمر الدولي حول النظام القانوني للمرفق العام الإلكتروني واقع تحديات وآفاق، أيام 26 و27 نوفمبر 2018، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف المسيلة، ص 11 و12

[2]- تنص المادة 1316-4 من القانون المدني الفرنسي على ما يلي:

(La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.

Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est

القانون التجاري الدولي للأمم المتحدة في قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، بخلاف ما كان عليه الأمر بالنسبة للكتابة الإلكترونية، بحيث اكتفى في التعريف المذكور أعلاه إلى تبيان الآثار القانونية للتوقيع الإلكتروني دون تبيان أو تحديد لأشكاله أو صوره، ويمكن تفسير ذلك على العموم في أن المشرع الفرنسي لا يفرق بين التوقيع الإلكتروني والتوقيع التقليدي من حيث وظائفه وآثاره القانونية، على الرغم الخصائص الكثيرة التي يتميز بها التوقيع الإلكتروني عن التوقيع التقليدي[1].

أما بخصوص المشرع الجزائري وبالعودة إلى نصوص القانون المدني الجزائري فإننا نجده قد أهمل تعريف التوقيع الإلكتروني، قبل أن يتدارك ذلك بإصداره للقانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[2]، الذي عرف التوقيع الإلكتروني بموجب المادة الثانية فقرة أولى بنصها على أن (التوقيع الإلكتروني بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق). كما عرف في الفقرة الثانية منها الموقع على أنه (شخص طبيعي يحوز بيانات إنشاء التوقيع الإلكتروني ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله). ويبدوا من خلال هذا التعريف أن المشرع الجزائري قد جمع بين الجانب التقني الوظيفي للتوقيع الإلكتروني إلا أنه أهمل تحديد الوسيلة التي يتم من خلالها اعتماد التوقيع الإلكتروني، كما أنه أهمل بيان أشكال التوقيع الإلكتروني وآثاره مكتفيا بالإشارة إلى ضرورة أن يتضمن التوقيع الإلكتروني بيانات في شكل إلكتروني دونما تحديد لشكل هذه البيانات أو الشكل الإلكتروني المشار إليهما في المادة الثانية فقرة أولى أعلاه.

---

présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Eta)،Article 1316-4 Créé par Loi n°2000-230 du 13 mars 2000 - art. 4 JORF 14 mars 2000 Abrogé par Ordonnance n°2016-131 du 10 février 2016 - art. 3

[1]- يتميز التوقيع الإلكتروني عن التوقيع التقليدي في أنه يرتبط برسالة إلكترونية، وفي أنه يحقق وظائف التوقيع التقليدي، والأمن والخصوصية، والسرعة. للمزيد حول هذا الموضوع راجع إيلاف فاخر كاظم علي، مخاطر العمليات المصرفية الإلكترونية (دراسة مقارنة)، المركز العربي للنشر والتوزيع، الطبعة الأولى، 2019، ص.ص 90-91

[2]- قانون رقم 15-04 مؤرخ في 01 فبراير 2015يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، منشور في الجريدة الرسمية العدد 06 مؤرخة في 10 فبراير 2015

كما يتضح من خلال هذا التعريف أن المشرع الجزائري قد تأثر إلى حد قريب بالتعريف الذي ساقته لجنة القانون التجاري الدولي للأمم المتحدة في قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية[1] الذي عرف التوقيع الإلكتروني في المادة 02 (أ) منه على أنه يعني (بيانات في شكل الكتروني مدرجة في رسالة بيانات، أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تُستخدم لتعيين هوية الموّقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموّقع على المعلومات الواردة في رسالة البيانات).

وبناء على ما سبق ذكره من تعريفات سواء لذلك التعريف الذي أورده المشرع الفرنسي أو الجزائري أو قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية إلى أنها تتفق جميعها على أن التماثل القائم في معنى كل من التوقيع الإلكتروني والتوقيع التقليدي، من حيث أنهما يعتبران وسيلة للتعبير عن الإرادة، يمكن من خلالهما تمييز هوية الملتزم بالتوقيع، فكما يتم استخدام التوقيع التقليدي للتصديق أو التوثيق للوفاء بتعاملات معينة ما ينشأ التزاما لدى الموقع على نحو لا يقبل التراجع أو النفي، فإن التوقيع الإلكتروني وعلى الرغم من أنه لا يتضمن القيام بتوقيع شيء ما باستخدام القلم والورقة وإرساله بعد ذلك عبر شبكة اتصال مؤتمنة، إلا أنه مثل التوقيع التقليدي يستخدم لتحديد هوية الموقع على معاملة ما[2].

ومن هذا الباب فإن التوقيع الإلكتروني يحوز نفس الحجية القانونية التي يحوزها التوقيع التقليدي في جميع التعاملات المدنية منها والإدارية، ومن ثمة فإنه يصلح لأن يكون دليلا للإثبات في منازعات العقود الإدارية المبرمة بالطريقة الإلكترونية، وما يؤكد ذلك هو نص المادة 07 من القرار الوزاري المؤرخ 17 نوفمبر 2013 المحدد لمحتوى البوابة الإلكترونية للصفقات العمومية وكيفيات تسييرها وكيفيات تبادل المعلومات بالطريقة الإلكترونية، التي نصت على ضرورة أن يصمم نظام المعلوماتية للصفقات العمومية في إطار احترام مبدأ سلامة الوثائق المتبادلة بالطريقة الإلكترونية، على نحو يضمن توقيع الوثائق بالطريقة الإلكترونية المؤمنة مع احترام الأحكام التشريعية والتنظيمية المعمول بها[3].

---

[1]- قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، اعتمد بتاريخ 05 يوليو 2001، تاريخ الاطلاع 17 إبريل 2020، منشور على الموقع الإلكتروني التالي:
https://uncitral.un.org/ar/texts/ecommerce/modellaw/electronic_signatures

[2]- عبد العزيز خنفوسي، قانون الدفع الإلكتروني، مركز الكتاب الأكاديمي، الأردن، 2018، ص 174

[3]- راجع المادة 07 من القرار الوزاري المؤرخ 17 نوفمبر 2013 المحدد لمحتوى البوابة الإلكترونية للصفقات العمومية وكيفيات تسييرها وكيفيات تبادل المعلومات بالطريقة الإلكترونية

2- شروط التوقيع الإلكتروني لإثبات العقد الإداري الإلكتروني

من خلال استقرائنا للنصوص القانونية المذكورة أعلاه في التشريع الوطني والتشريعات المقارنة الأخرى التي منحت للتوقيع الإلكتروني حجية قانونية كدليل للإثبات في المعاملات سواء المدنية منها أو الإدارية، نجد بأنها قد فرضت ضرورة توافر مجموعة من الشروط لأجل أن تكون قابلة للإعتداد بها كدليل لإثبات تلك المعاملات، يمكن إجمالها عموما في شرطين أساسيين يتعلق الشرط الأول بضرورة أن يكون التوقيع الإلكتروني مميزا لهوية صاحبه، أما الشرط الثاني فيتعلق بضرورة أن يكون التوقيع مقروءا ومتصفا بالاستمرارية، أما الشرط الثالث فيرتبط بضرورة إتصال التوقيع الإلكتروني بمحرر كتابي. وفيما يلي سيتم التفصيل في كل شرط من هذه الشروط على حدة.

أ- أن يكون التوقيع الإلكتروني مميزا لهوية صاحبه

يتصل هذا الشرط بوظيفة التوقيع في حد ذاتها التي تكمن في تحديد هوية الموقع الذي يستند إليه الدليل أو المستند، باعتباره وسيلة للتعبير عن إرادة الموقع في الإلتزام بما وقع عليه[1]. ومعنى ذلك أنه يشترط في التوقيع الإلكتروني كدليل للإثبات في منازعات العقود الإدارية المبرمة بالطريقة الإلكترونية أن يكون قابلا لأن ينسب لمتعامل إقتصادي معين.

فبالنسبة لدعاوى منازعات العقود الإدارية يمكن التحقق من مدى توافر شرطي الأهلية والصفة في المدعى والمدعى عليه من خلال التوقيع الإلكتروني الذي يبين هوية كل منهما وأهليته وصفته، كون الموقع تمنح له شهادة تبين ذلك، تعتمد من خلالها الجهة التي منحتها صحة المعلومات الواردة فيها[2]، وهي شهادة تصدر أثناء عملية إنشاء التوقيع الإلكتروني من شأنها إثبات هوية الموقع[3].

ولقد أشار المشرع الفرنسي إلى هذا الشرط في المادة 1316-4من القانون المدني التي نصت على أن التوقيع الإلكتروني هو ذلك التوقيع الذي يؤكد شخصية صاحبه وصحة الواقعة المنسوبة إليه حتى يثبت عكس ذلك، على أن تكون الوسيلة المستخدمة في التوقيع الإلكتروني

---

[1]- محمود عبد السلام علي، الحملات الإعلانية، دار المعتز للنشر والتوزيع، الطبعة الأولى، الأردن، 2017، ص 362

[2]- نادية أو طالب، المحاكم الإلكترونية إجراءاتها ومدى قانونية تطبيقها في الأردن، دراسات للنشر والتوزيع، الأردن، 2018، ص 40

[3]- فيصل عبد الحافظ الشوابكة، النظام القانوني للعقد الإداري الإلكتروني، مجلة الجامعة الإسلامية للدراسات الاقتصادية والإدارية، المجلد 21، العدد الثاني، يونيو 2013، ص 357

مقبولة وموثوقا بها، بحيث تضمن اتصال التوقيع بالعمل أو المستند المرتبط به لإتمام التصرف القانوني، بما يعبر عن رضا الأطراف بالالتزامات المترتبة عن هذا التصرف، وتؤكد شخصية صاحبه وصحة الواقعة المنسوبة إليه حتى يثبت عكس ذلك[1].

كما أقر المشرع الجزائري بدوره هذا الشرط كذلك بموجب المادة 323 مكرر 1 من القانون المدني التي وضعت شرط إمكانية التأكد من هوية الشخص الموقع، للإحتجاج بالتوقيع الإلكتروني كدليل إثبات. وهو ما يستفاد كذلك من نص المادة 06 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين التي نصت على وظيفة التوقيع الإلكتروني، من حيث أنه يستعمل لتوثيق هوية الموقع.

ويبدو أن هذا الشرط ينطبق بدوره كذلك حتى في المعاملات الإدارية وبوجه خاص العقود الإدارية، بحيث نجد المشرع الجزائري قد حرص على التأكيد على ضرورة أن يعبر التوقيع الإلكتروني على هوية صاحبه في إطار الصفقات العمومية المبرمة بالطريقة الإلكترونية، وما يؤكد ذلك هو نص المادة 07 من القرار الوزاري المؤرخ 17 نوفمبر 2013 المحدد لمحتوى البوابة الإلكترونية للصفقات العمومية وكيفيات تسييرها وكيفيات تبادل المعلومات بالطريقة الإلكترونية، التي أوجبت ضرورة أن يصمم نظام المعلومات للصفقات العمومية في إطار احترام مبدئ سلامة الوثائق المتبادلة بالطريقة الإلكترونية على نحو يضمن التعرف على هوية المتعاملين الاقتصاديين والتأكد منها[2].

---

[1]- تنص المادة 1316-4 من القانون المدني الفرنسي على ما يلي:

(La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.

Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Eta).Article 1316-4 Créé par Loi n°2000-230 du 13 mars 2000 - art. 4 JORF 14 mars 2000 Abrogé par Ordonnance n°2016-131 du 10 février 2016 - art. 3

[2]- راجع المادة 07 من القرار الوزاري المؤرخ 17 نوفمبر 2013 المحدد لمحتوى البوابة الإلكترونية للصفقات العمومية وكيفيات تسييرها وكيفيات تبادل المعلومات بالطريقة الإلكترونية

ب- قابلية التوقيع الإلكتروني للقراءة والاستمرارية

يعتبر التوقيع الإلكتروني جزءا لا يتجزأ من المحرر الإلكتروني، بحيث يتصل به اتصالا ماديا ومباشرا بما يدل على رضا موقعه وقبوله لمضمون المحرر، بمجرد توقيعه بالشكل الإلكتروني على البيانات التي تحتويها المحررات الإلكترونية، وهو بذلك يمثل صورة من صور الكتابة، حيث يأخذ التوقيع الإلكتروني شكل أرقام سرية أو رموز محددة تدل على موافقة صاحبها على البيانات والمعلومات التي وقع عليها[1].

ومن هذا الباب فإنه يشترط في التوقيع الإلكتروني ما يشترط في الكتابة الإلكترونية من حيث قابليته للقراءة والفهم والوضوح، وقابليته للحفظ والاستمرار، على نحو يمكن القاضي الإداري من الرجوع إليه طيلة الفترة التي يستخدم فيها كدليل للإثبات، وهو ما يستفاد من نص المادة 323 مكرر 1 من القانون المدني التي وضعت شرط قابلية الكتابة الإلكترونية للحفظ ظروف تضمن سلامتها، للإحتجاج بها بوجه عام وبالتوقيع الإلكتروني بوجه خاص كدليل إثبات، بالإضافة إلى نص المادة 06 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين التي نصت على ضرورة أن تحفظ الوثيقة الموقعة إلكترونيا في شكلها الأصلي.

كما يجد هذا الشرط مصدره في إطار المعاملات الإدارية ضمن نص المادة 07 من القرار الوزاري المؤرخ 17 نوفمبر 2013 المحدد لمحتوى البوابة الإلكترونية للصفقات العمومية وكيفيات تسييرها وكيفيات تبادل المعلومات بالطريقة الإلكترونية، التي أوجبت ضرورة أن يصمم نظام المعلومات للصفقات العمومية في إطار احترام مبدئ سلامة الوثائق المتبادلة بالطريقة الإلكترونية على النحو الذي يجب أن تضمن من خلاله صيغ وأشكال رقمنة الوثائق المكتوبة عدم المساس بسلامتها[2].

وبالنتيجة عن ذلك فإنه ومتى تم الإلتزام بالشروط المبينة أعلاه سواء الواردة في التشريع المنظم للمعاملات المدنية أو الإدارية، حاز التوقيع الإلكترونية على حجية قانونية تجعله قابلا للإعتداد به كدليل إثبات في منازعات العقود الإدارية المبرمة بالطريقة الإلكترونية، وهو ما يستفاد كذلك من القرار الصادر عن مجلس الدولة الفرنسي بتاريخ 30 مارس 2001 الذي جاء

---

[1]- أسامة بن غانم العبيدي، حجية التوقيع الإلكتروني في الإثبات، المجلة العربية للدراسات الأمنية والتدريب، المجلد 28، العدد 56، ص 09

[2]- راجع المادة 07 من القرار الوزاري المؤرخ 17 نوفمبر 2013 المحدد لمحتوى البوابة الإلكترونية للصفقات العمومية وكيفيات تسييرها وكيفيات تبادل المعلومات بالطريقة الإلكترونية

فيه بأن (لتوقيع الإلكتروني مجموعة من البيانات تصدر عن شخص نتيجة للالتزام بالشروط الواردة في الفقرة الثانية من المادة 4/1316 من القانون المدني الفرنسي)[1].

الخاتمة:

من خلال دراستنا لموضوع خصوصية الإثبات في منازعات العقود الإدارية المبرمة بالطريقة الإلكترونية حالة الصفقات العمومية الإلكترونية، يمكن أن نشير إلى أهم النتائج التي خلصت إليها هذه الدراسة:

- أنه من منطلق أن المشرع الجزائري قد أجاز إبرام العقود الإدارية بالطريقة الإلكترونية باتباع إجراءات قانونية معينة تضمنها المرسوم الرئاسي رقم 15-247 وكذا القرار الوزاري المؤرخ 17 نوفمبر 2013 المحدد لمحتوى البوابة الإلكترونية للصفقات العمومية وكيفيات تسييرها وكيفيات تبادل المعلومات بالطريقة الإلكترونية، فإنه ينجم عن ذلك عديد الآثار القانونية التي تسمح بإمكانية الإعتداد بالمحررات الإلكترونية المنبثقة عن هذا النوع من المعاملات الإدارية.
- أن هذا التطور المستمر قد دفع المشرع الجزائري كغيره من التشريعات المقارنة إلى تنظيم هذا الشكل المستجد من التعاملات الإلكترونية، من خلال تبيان وسائل الإثبات في العقود المدنية أو الإدارية المبرمة بالطريقة الإلكترونية، التي تعتبر فيهما المحررات الإلكترونية المتمثلة في الكتابة الإلكترونية والتوقيع الإلكتروني أحد أهم وسائل الإثبات التي يمكن للقاضي الإداري الإستعانة بها للفصل في منازعات العقود الإدارية المبرمة بالطريقة الإلكترونية.
- أن المشرع الجزائري لم يبين في المرسوم الرئاسي رقم 15-247 ولا القرار الوزاري الصادر بتاريخ درجة حجية المحررات الإلكترونية في المعاملات الإدارية على غرار المعاملات المدنية في القانون المدني درءا لأي تأويل، طالما أنه قد أقر بإمكانية إبرام العقود الإدارية بالطريقة الإلكترونية، فلا نكاد نلمس نصا قانونيا صريحا يشير إلى حجية المحررات الإلكترونية التي يجري تبادلها بين المصالح المتعاقدة والمتعاملين الاقتصاديين في البوابة الإلكترونية للصفقات العمومية، وإن كانت بعض نصوصه تشير ضمنا إلى ذلك.

---

[1]- عصمت عبد المجيد بكر، دور التقنيات العلمية في تطور العقد، دار الكتب العلمية، لبنان، 2015، ص 347

- أن المحررات الإلكترونية في مجال العقود الإدارية المبرمة بالطريقة الإلكترونية تتمتع بذات الحجة القانونية التي تتمتع بها تلك المحررات في المعاملات المدنية بموجب أحكام وقواعد القانون المدني، ما دامت تلك القواعد لا تتعارض مع طبيعة وخصوصية الروابط القانونية الناشئة في مجال القانون العام.
- أن الحجية القانونية التي تتمتع بها المحررات الإلكترونية في المعاملات الإدارية شأنها في ذلك شان المعاملات المدنية، مرتبطة بضرورة توافر مجموعة من الشروط حتى تكون قابلة للإعتداد بها كدليل لإثبات في منازعات العقود الإدارية المبرمة بالطريقة الإلكترونية.



المحور الرابع

الجريمة الماسة بالقطاع الخدماتي

دور الوسائط الالكترونية في تنامي جريمة تبييض الأموال

The role of electronic media in the growing crime of money laundering

د.دربال سهام أستاذة مساعدة قسم "ب"
معهد الحقوق و العلوم السياسية
– المركز الجامعي مغنية- الجزائر

مقدمة:

تعتبر جريمة تبييض الأموال من أخطر الممارسات التي تمس اقتصاديات الدول لما تسببه من أضرار اقتصادية وجنائية و اجتماعية على المستوى المحلي و الدولي.

و ظهرن هذه الجريمة لأول مرة في الولايات المتحدة الأمريكية خلال الفترة من 1920_1930م ، حيث لجأت عصابات المافيا إلى إنشاء محلات لغسل الملابس الاتوماتيكية، من اجل استثمار الأموال التي تحصلت عليها بطرق غير مشروعة من تجارة المخدرات بغية إخفاء أصل هذه الأموال[1].

و جريمة تبييض الأموال بوسائلها الفنية الحديثة قد تم ممارستها بشكل منظم سنة 1932بواسطة "Meyer Lansky" ، و الذي كان يمثل آنذاك حلقة الوصل بين المافيا الأمريكية و المافيا الإيطالية بصقلية ، و ذلك من اجل تسهيل دخول القوات البحرية للحلفاء إلى الجزيرة، ومن أجل ذلك كان يتم اللجوء الى البنوك السويسرية لإمكان إخراج النقود من الولايات المتحدة الأمريكية و إيداعها في حسابات رقية بسويسرا من خلال القروض الوهمية و كذلك الاستثمارات المباشرة التي تتم بواسطة وهمية.[2]

و قد عرفت هذه الجريمة انتشارا واسعا في الوقت الراهن؛ ويرجع ذلك إلى ارتكابها باستخدام وسائل تقنية حديثة، تتسم بالسرعة فمما لاشك فيه أن التطور التكنولوجي ساهم في تطور صور

[1] عبد الفتاح سليمان، مكافحة غسل الأموال، دار الكتب القانونية، مصر ، 2006،ص.15.

[2] محمد علي سكيكر، مكافحة جريمة غسل الأموال على المستويين المصري و العالمي ، دار الجامعة الجديدة، 2007 ص.08.

هذه الجريمة فقد ظهرت العديد من التقنيات التي غيرت في السلوك الإجرامي للأشخاص ، فتم رصد طرق جديدة و متنوعة لتبييض الأموال .

و الواقع أن الوسائط الالكترونية لها تأثير كبير و سلبي في انتشار هذا النوع من الجرائم. لذلك تهدف هذه الدراسة إلى الإجابة عن الإشكالية التالية: ما المقصود بجريمة تبييض الأموال و ما مدى تأثرها بالوسائط الالكترونية ؟.

و للإجابة عن هذه الإشكالية نقسم دراستنا الى قسمين :

الأول نتطرق فيه إلى المدلول القانوني لجريمة تبييض الأموال.

و الثاني حول تأثير الوسائط الالكترونية في جريمة تبييض الأموال.

أولا : المدلول القانوني لجريمة تبييض الأموال

تعتبر جريمة تبييض الأموال من الجرائم الاقتصادية فهي ترتبط بالبنوك و المؤسسات المالية لما توفره عملياتها من أساليب تستخدم في تبييض الأموال .

1. تعريف تبييض الأموال

هو عبارة عن عملية أو عدة عمليات يتم من خلالها إضفاء الصفة المشروعة على أموال ناتجة عن القيام بأفعال غير مشروعة قانونا، تكون في الغالب أفعالا إجرامية قام بها الجاني و لجأ إليها من اجل إخفاء جرائمه التي حصلت نتيجة ارتكابه لها على الأموال محل جريمة تبييض الأموال[1].

كما عرفها البعض بأنها عبارة عن فعل أو مجموعة من الأفعال أو المساهمة فيها عن قصد بهدف إضفاء الصفة الشرعية على أموال تم اكتسابها بطريقة غير مشروعة بارتكاب جناية أو جنحة معاقب عليها في التشريع الوطني أو الأجنبي[2].

بالنسبة لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة غير الوطنية فعرفتها بأنها " تحويل الممتلكات أو نقلها، مع العلم بأنها عادات جرائم، بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات أو مساعدة أي شخص ضالع في ارتكاب الجرم الأصلي الذي تأتت منه على الإفلات من العواقب القانونية لفعلته؛

---

[1] محمد علي سكيكر، المرجع السابق ، ص.07؛ راجع في ذات المعنى: السيد عبد الوهاب عرفة، الوجيز في مكافحة جريمة غسل الأموال ،دار المطبوعات الجامعية،2005،ص.11.

[2] امجد سعود قطيفان الخريشة، جريمة غسيل الأموال -دراسة مقارنة-، الطبعة الأولى،دار الثقافة، 2006،ص.32.

إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو ملكيتها أو الحقوق المتعلقة بها، مع العلم بأنها عائدات جرائم" .[1]

أما المشرع الجزائري فلم يعرف جريمة تبييض الأموال بل اكتفى بتحديد الأفعال التي تشكل هذه الجريمة في المادة الثانية من القانون 05 -01[2]و المادة 389 مكرر من قانون العقوبات[3]التي تنص على " يعتبر تبييضا للأموال:

أ - تحويل الممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية، بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات، على الإفلات من الآثار القانونية لفعلته.

.ب - إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها، مع علم الفاعل أنها عائدات إجرامية.

ج- اكتساب الممتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك وقت تلقيها، أنها تشكل عائدات إجرامية.

د- المشاركة في ارتكاب أي من الجرائم المقررة وفقا لهذه المادة، أو التواطؤ أو التآمر على ارتكابها ومحاولة ارتكابها والمساعدة والتحريض على ذلك وتسهيله وإسداء المشورة بشأنه.

ولا يختلف مفهوم جريمة تبييض الأموال الالكترونية عن جريمة تبييض الأموال العادية فيقصد بها : "مجموعة الأفعال التي تهدف الى إخفاء المصدر غير المشروع للأموال المتحصل عليها بطرق غير مشروعة كالمخدرات و الاتجار بالبشر و غيرها باستعمال الانترنت من اجل إضفاء صفة الشرعية على هذه الأموال ".

2. أركان جريمة تبييض الأموال

تعتبر اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع في المخدرات و المؤثرات العقلية "اتفاقية فيينا 1988" الخطوة الأولى التي جسدت قناعة المجتمع الدولي بضرورة مكافحة عمليات تبييض الأموال، من خلال تبني سياسة جنائية واضحة بخصوص مكافحة تبييض الأموال، على الرغم من ان الاتفاقية لم تستخدم مصطلح تبييض الأموال في أي من موادها بطريقة مباشرة ، هذا

[1]اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية ، 15 نوفمبر 2000.
http://hrlibrary.umn.edu/arab/CorgCRIME.html

[2]القانون 05 -01 المؤرخ 6 فبراير 2005 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما

[3]القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم لقانون العقوبات الجزائري .

وقد فرضت على الدول الأعضاء التزاما يقضي بتجريم سلوكيات تنطوي على تبييض الأموال الناتجة عن الاتجار غير المشروع بالمخدرات .[1]

وجريمة تبييض الأموال باعتبار انها وصفا جنائيا مستقلا عن غيره من الاوصاف يستوجب منا التعرض لأركان هذه الجريمة.

فجريمة تبييض الأموال كغيرها من الجرائم لابد أن تتبلور ماديا و تتخذ شكلا معينا و هو الركن المادي للجريمة، إلا أن هذا الأخير لا يكفي لإسناد المسؤولية إلى شخص معين بل يجب أن يتولد لديه النية الإجرامية و التي تشكل الركن المعنوي للجريمة بالإضافة إلى ضرورة وجود نص قانوني يجرم الفعل إذ لا جريمة بدون نص قانوني.[2]

1) الركن الشرعي

لا تقوم الجريمة إلا إذا كان الفعل المرتكب مشروعا، فالركن الشرعي يقوم على النص الشرعي الذي يجرم الفعل و يحدد عقوباته[3]، وعليه قد جرم المشرع الجزائري الأفعال المكونة لجريمة تبييض الأموال المادة الثانية من القانون 05 -01[4] و المادة 389 مكرر السالفة الذكر .

2) الركن المادي

إن تبييض الأموال هي جريمة تهدف إلى إضفاء طابع الشرعية على الأموال ذات المصدر الإجرامي ، و هي بذلك جريمة تبعية تفترض لاكتمال بنيانها القانوني وقوع جريمة سابقة عليها ، هي الجريمة الأصلية او الجريمة الأولية تكون مصدر الأموال المراد تبييضها مثل جريمة المتاجرة بالمخدرات أو التهريب أو الاتجار بالأسلحة ...

لذلك يمكن القول إن جريمة تبييض الأموال تتكون من عنصرين

أولا: الحصول على الأموال من مصدر إجرامي و هو ما يعرف أيضا بالركن المفترض او الركن الخاص .[5]

---

[1] امجد سعود قطيفان الخريشة ، المرجع السابق ، ص.90.

[2] راجع :أحمد بوسقيعة ، الوجيز في القانون الجزائي العام ، دار هومة ، الطبعة الرابعة ، 2007، ص.48.

[3] تنص المادة الأولى من قانون " لا جريمة و لا عقوبة او تدابير امن بغير قانون "

[4] القانون 05 -01 المؤرخ 6 فبراير 2005 السالف الذكر

[5] خوجة جمال ،جريمة تبييض الأموال -دراسة مقارنة-، مذكرة ماجستير، كلية الحقوق و العلوم السياسية ، جامعة تلمسان، 2007-2008 ، ص.76.

وقد تطرق المشرع الجزائري له في المادة 389 مكرر من قانون العقوبات الجزائري "....تحويل الممتلكات او نقلها مع علم الفاعل بأنها عائدات إجرامية...." والمادة الثانية من القانون 05-01 المتعلق بالوقاية من تبييض الأموال "

ويفهم من هذه المواد أن المشرع وسع في نطاق التجريم حيث جاء النص مناسبا لطبيعة هذه الظاهرة الإجرامية التي تتغير أساليب وكيفيات ارتكابها.

ثانيا : الشروع أو إتمام عملية التبييض يقصد بها القيام بالسلوك المادي الذي بمقتضاه تكتسي العائدات الإجرامية صفة أو مصدر وهمي مشروع يبيح لحائزها التصرف فيها بكل حرية لاحقا [1].

3) الركن المعنوي

إضافة إلى تحقق الركن المادي لابد من توافر الركن المعنوي، و تختلف التشريعات فيما بينها ، حيث يتطلب البعض القصد الجنائي في جميع صور السلوك الإجرامي الذي يندرج في إطار تبييض الأموال كالمشرع الفرنسي، و تشريعات أخرى تجيز وقوعها بالخطأ إلى جانب القصد الجنائي العام كالتشريع الألماني ، على ان هناك بعض التشريعات تطلب القصد الجنائي الخاص بالإضافة إلى القصد العام.[2]

بالنسبة للمشرع الجزائري وبالرجوع إلى المادة 389 مكرر من قانون العقوبات و ما يليها نجد انه اعتبر جريمة تبييض الأموال من الجرائم العمدية التي تتطلب القصد الجنائي العام و الخاص، و منه لا يمكن تصور قيام هذه الجريمة الا بإرادة الجاني من جهة و العلم بالأموال غير المشروعة محل جريمة تبييض الأموال من جهة أخر.

ثانيا : تأثير الوسائط الالكترونية في جريمة تبييض الأموال

ان ثورة الاتصالات في العالم خلال العقدين الأخيرين رافقها انتشار لظاهرة الجريمة عالميا، وجريمة تبييض الأموال من بين هذه الجرائم، حيث يستفيد مبيضو الأموال من الحدود المفتوحة بين الدول، ومن المزايا التي توفرها تكنولوجيا الاتصال لهذه الجريمة استعمال تقنيات تحويل

---

[1] خوجة جمال ، المرجع السابق، ص.79.

[2] امجد سعود قطيفان الخريشة ، المرجع السابق ، ص.114.

الأموال القذرة من بلد لآخر لإبعادها عن الشبهة و المصادرة، كما تميز بسرعة الانتشار الجغرافي في ظل العولمة و تدويل التبادلات المالية و التجارة الدولية.[1]

تستخدم شبكة الانترنت بما توفره من سهولة في انتشار جريمة تبييض الأموال؛ و هناك العديد من الوسائط الالكترونية التي تستخدم في ذلك لعل أهمها بنوك الانترنت[2]، بطاقات الدفع الالكتروني[3]، النفوذ الالكترونية [4]، و الشيك الالكتروني، و تداول الأموال في صورة أسهم وسندات عبر شبكة الانترنت ، و التعامل ببطاقة "موندكس". وسنتكفي بدراسة تبييض الأموال باستعمال الشيك الالكتروني؛ عن طريق الأسهم و السندات التي يتم تداولها عبر شبكة الانترنت ؛ تبييض الأموال باستخدام بطاقة موندكس.

1.الشيك الالكتروني

يعتبر من أهم وسائل الدفع الالكترونية و الذي يتناسب و التجارة و يعد من أكثر الأوراق التجارية الالكترونية الذي يتماشى و تقنية المعلومات و المعالجة الآلية، فالبنوك تعتبر طرفا أساسيا في الوفاء بها و تحصيلها و بما ان الشيكات لابد من أن تكون على نموذج بنكي هذا يسمح للبنوك بوضع نماذج تتلاءم و المعالجة الآلية للبيانات [5]

---

[1]نادية عبد الرحيم،؛ أمين بن سعيد، جريمة تبييض الأموال في ظل رقمنة الخدمات المصرفية ، مجلة الدراسات الاقتصادية و المالية، العدد10،الجزء الثاني، جامعة الوادي ،2017،ص.31.

[2]هي صورة من صور التجارة الالكترونية و هذه البنوك ليست بنوكا في الواقع بالمعنى المألوف فهي لا تقوم بقبول الودائع مثلا او تقديم تسهيلات مصرفية، و لكنها عبارة عن وسيط في القيام ببعض العمليات المالية و ذلك باستخدام ما يعرف بالنقود الالكترونية، فيقوم المتعامل بإدخال الشفرة السرية من ارقام او خلافه بطباعتها على الكمبيوتر و من ثم يستطيع تحويل الأموال بالطريقة التي يأمر بها الجهاز ، و تعرف هذه الطريقة باسم عمليات التحويل عبر الانترنت، و تتيح لمبيضي الأموال تحويل كميات ضخمة من الأموال بسعة و امان؛ عمرو عيسى الفقي، مكافحة غسيل الأموال في الدول العربية، الطبعة الأولى، المكتب الجامعي الحديث، 2005،ص.127.

[3]عرفها المشرع الجزائري في المادة 543 مكرر23 من القانون التجاري التي تنص على" تعتبر بطاقة دفع كل بطاقة صادرة عن البنوك و الهيئات المالية المؤهلة قانونا و تسمح لصاحبها بسحب او تحويل أموال ".

[4]هي نقود محمية بفعل التشفير الممنوح من المصارف للعملاء على العمليات المالية التي يقومون بها ، و تصبح كالنقود الورقية ملك لحائزها يتعامل بها كيفما يشاء دون فرض الرقابة عليها ، و بها تجري عمليات تبييض الأموال دون كشفها من المصالح الأمنية؛ هيثم عبد الرحمان البقلي، غسيل الأموال كإحدى عمليات الجريمة المنظمة بين الشريعة و القانون المقارن، دار العلوم،ص.59.

[5]باطلي غنية ، وسائل الدفع الالكترونية ، الطبعة الأولى ، دار هومة ،2018، ص.245.

و يعرف الشيك الالكتروني بأنه رسالة الكترونية مؤمنة و موثقة يرسلها مصدر الشيك الى مستلمه "الحامل" ليعتمده و يقدمه للبنك الذي يعمل على الانترنت، ليقوم البنك بتحويل قيمة الشيك الى حساب الحامل، و بعد ذلك يقوم بإلغاء الشيك و إعادته الكترونيا إلى مسلم الشيك ليكون دليلا على انه قد تم صرف الشيك فعلا و يمكن له ان يتأكد الكترونيا من أنه بالفعل قد تم تحويل المبلغ الى حسابه.[1]

والحقيقة ان علاقة الشيك الالكتروني بجريمة تبييض الأموال هي علاقة وثيقة و مباشرة، فالشيك الالكتروني يعتمد على وجود حساب عادي للعميل أو لمحرر الشيك لدى احد البنوك ثم يقوم العميل بنقل الحساب و تداوله عبر شبكة الانترنت في صفقات تجارية يكون طرفا فيها، و يكون الشيك الالكتروني هو وسيلة التداول و قبل ذلك يكون العميل هو الوسيط بين مصدر الشيك و محرره "الساحب" و بين المستفيد.[2]

و بالتالي صار من السهل على مبيضي الأموال اجراء العديد من العمليات المصرفية و تحويل الأموال غير المشروعية بسهولة في وقت وجيز .

فمثلا إذا كان للشخص أموالا غير مشروعة مهما كان مصدرها ، أودعها لدى البنك و أراد تبييضها بطريقة الشيك الالكتروني فيقوم بمعاملة بيع او إيجار... مع أشخاص آخرين عن طريق شبكة الانترنت ، و يسدد لهم عن طريق الشيك الالكتروني فيخرج المال غير المشروع من ذمة الشخص إلى ذمة من تعامل معهم بالبيع أو الإيجار....

وهذه العمليات تتسم بالدقة والسرية فالبنك المودع لن يسأل عن مصدر الأموال و العملاء كذلك الذين يتم التعامل معهم لن يسألوا عن مصدر المال المحول إليهم كمستفيدين عن طريق الشيك الالكتروني الصادر من العميل الذي بدأت المعاملة من طرفه.[3]

---

[1]باطلي غنية، المرجع نفسه، ص.246، لا يختلف مفهوم الشيك الالكتروني عن الشيك العادي كثيرا فيقصد بهذا الأخير انه" محرر بموجبه يعطي الساحب الى المسحوب عليه و الذي لا يمكن الا ان يكون بنكا او مؤسسة عمومية مؤهلة قانونا لمسك حسابات الشيكات ، امر بالوفاء لدى الاطلاع بمبلغ محدد من النقود للمستفيد او لأمره او سند مكتوب و مسحوب على بنك او مؤسسة مالية مؤهلة قانونا و يسمح بحصول الوفاء لمصلحة حامله بمبلغ من النقود . عبد الله ليندة ، مواجهة تبييض الأموال عن طريق وسائل الدفع ، رسالة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تيزي وزو ، 2019، ص.30.

[2]عبد الفتاح بيومي حجازي، جريمة غسيل الامول عبر شبكة الانترنت-دراسة متعمقة عن جريمة غسل الأموال عبر الوسائط الالكترونية في التشريعات المقارنة-، الطبعة الأولى ، 2009، ص.98.

[3]عبد الفتاح بيومي حجازي،المرجع السابق،ص.98.

فسهولة التعامل بالشيك الالكتروني فتح المجال اما المجرمين لاستعماله في تنفيذ عمليات تبييض الأموال . و عليه فان التكنولوجيا الحديثة لعبت دورا هاما في انتشار الفساد المالي و الإداري في العديد من المنشآت الاقتصادية في مختلف دول العالم ،و في المساعدة على إخفاء الجريمة الاقتصادية و صعوبة تعقبها لانعدام الأدلة وهو ما جعل البعض يطلق تسمية "الغسيل الشيطاني" على عمليات تبييض الأموال.[1]

2.تبييض الأموال من خلال تداول الأسهم و السندات عبر شبكة الانترنت

تعدّ بورصة الأوراق المالية المكان الذي يلتقي فيه مختلف المستثمرين، لكونها مركزاً تتقابل فيه الشركات التي تبحث عن الأموال والراغبون في استثمار أموالهم، كما تجد المشروعات رؤوس الأموال اللازمة ببورصة الأوراق المالية التي تعتبر شريان الحياة بالنسبة لاقتصاد البلاد في توجيه المدّخرات إلى الإنتاجية[2].

فيتم تبييض الأموال في هذه الحالة عن طريق اجراء عمليات شراء و بيع للأوراق المالية التي تتم بين مضاربين يتم التواطؤ بينهم، بحيث تتم إدارة حساباتهم عن طريق سمسار واحد و مثال ذلك: يقوم هذا السمسار بشراء صفقة من احد البورصات في دولة ما و لتكن من إنجلترا لحساب عميل اخر في إيطاليا بفائدة معينة ،ثم يقوم بإعادة بيعها مرة أخرى بقيمة أزيد من قيمة الشراء، ثم يقوم بإعادة بيعها مرة أخرى بسعر اقل من سعر العميل السابق ،بحيث يتضح خسارة العميل السابق و تحقيق مكسب للعميل الأول ، و يكون فرق المكسب لهذا العميل هو قيمة المال الذي تم غسله دون ظهور علاقة بين العميل الأول و الأخير.[3]

و مما لاشك فيه ان سوق البورصة من مجالات الاستثمار الجاذبة لمبيضي الأموال نظرا لتداول رأس المال بسرعة و سهولة ، سيما لو كان بوسيلة الكترونية هي شبكة الانترنت، حيث يلجا مبيض الأموال الى شراء مجموعة كبيرة من الأسهم و السندات بأموال ذات المصدر غير المشروع ا، و المضاربة في البورصة على سلعة ثم يقوم بتحريك السلعة او الأسهم أو السندات و بيعها ،و إعادة شراءها حتى يتم تدويرها و تبييضها، و ذلك ممكن و سهل لو تم بوسيلة الكترونية في شبكة

[1] عبد الفتاح بيومي حجازي،المرجع نفسه ،ص.99.

[2] محمد سعيد عبد العاطي، جرائم البورصة- دراسة مقارنة بين القانون الفرنسي والمصري-، دار النهضة العربية، القاهرة، 2013، ص.09.

[3] محمد علي سكيكر ، المرجع السابق ،ص.73.

انترنت من خلال التعامل على مواقع البورصات الافتراضية او البورصات العالمية و التي لها مواقع على شبكة الانترنت .[1]

و بناء على ما سبق يمكن القول ان الأوراق المالية التي يتم تداولها في سوق البورصة من اهم الأدوات التي يستغلها مبيضو الأموال، حيث يقومون بتبييض أموالهم عن طريق الاستثمار بشراء الأسهم و السندات، و طرحها للتداول في البورصات التي لها مواقع عبر شبكة الانترنت و عند استعمال هذه الا وراق المالية لا يسأل الوسطاء الماليون و لا العملاء عن مصدر هذه الأموال.

3.استخدام بطاقة موندكس« MONDEX »في تبييض الأموال

يمكن استخدام بطاقة "موندكس"في المعاملات اليومية البسيطة، و يعمل نظامها على تقنية البطاقة الذكية و تستخدم حساب كحساب المدين العادي او بطاقة الأئتمان التي تخزن المعلومات على الشريحة الالكترونية و التي تحتوي على محفظة نقود الكترونية تسجل عليها قيمة البطاقة؛ المحفظة مقسمة الى خمس أقسام تسمح باستعمال خمس أنواع من العملات في وقت واحد، كما تحتوي الشريحة على برامج الامن التي تحمي العمليات بين بطاقة "موندكس" و بطاقات أخرى[2].

تسمح تقنية""موندكس للمستخدمين تحويل الأموال غير المشروعة عبر جهاز مودم أو عبر انترنت، مع ضمان تشفير امن لعمليات تبييض الأموال، دون أن تترك أثارا تمكن من التعرف على مرتكبيها.

وتميز تقنية "موندكس" في تبييض الأموال بالابتعاد عن القطاع المصرفي الحكومي أو الخدمات المصرفية التقليدية وسهولة تجاوزها للحدود الجغرافية، مما يجعل عملية تتبعها امرا مستحيلا، ويشكل مشكلة قانونية للتشريعات التقليدية، الأمر الذي يحتم على الدول إعادة النظر في تشريعاتها لمواكبة التطورات التكنولوجية وعقد الاتفاقيات الدولية لمواجهة هذه الظاهرة.[3]

خاتمة :

من خلال ما سبق يمكن القول ان جريمة تبييض الأموال الالكترونية لا تختلف عن جرائم تبييض الأموال التقليدية كون أنهما يتفقان في المفهوم القانوني، والاختلاف الجوهري بينهما

[1] عبد الفتاح بيومي حجازي، المرجع السابق،ص.102.

[2] مسعودي عبد الهادى، الاعمال المصرفية الالكترونية ،دار اليازوري، ص.98.

[3] نعيم سلامة القاضي؛ أيمن أبو الحاج ،موسي سعيد مطر؛ مشهور هذلول بربور، البنوك و عمليات غسيل الأموال، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد الثالث و الثلاثون، 2012.ص.359.

يكمن في ان جريمة تبييض الأموال الالكترونية يستخدم فيها الجناة شبكة الانترنت كأداة لإخفاء مصدر الأموال غير المشروع.

و الحقيقة أن أساليب ارتكاب هذه الجريمة تطورت بشكل كبير حيث تم استغلال العديد من الوسائط الالكترونية كالشيكات الالكترونية، و تداول الأسهم و السندات في البورصات التي لها مواقع في شبكة الانترنت ، بالإضافة الى استعمال تقنية موندكس، و غيرها من الوسائط فبات من السهل على الجاني الهروب من المتابعة القانونية.

ان جريمة تبييض الأموال الالكترونية تعتبر من أهم التحديات التي تقف ضد الاستقرار الاقتصادي و المالي للدول لما لها من آثار سلبية ، و لا يمكن انكار صعوبة إيقاف الجناة في هذا النوع من الجرائم ؛ و تكمن الصعوبة في استحالة السيطرة او مراقبة جميع المعاملات المالية الالكترونية .



المحور الخامس

أثر الجريمة المعلوماتية على الاقتصاد

انعكاسات الجريمة المعلوماتية على الاقتصاد

The effects of information crime on the economy

د. مجدوب نوال أستاذة محاضرة قسم - ب
المركز الجامعي مغنية الجزائر

تمهيد :

لا يمكن إنكار المزايا التي قدمتها تكنولوجيا الإعلام و الاتصال في كافة مجالات الحياة [1] إذ شهد العالم اليوم ثورة هائلة في مجال تقنية المعلومات، و التي أصبحت من أساسيات الحياة و سمة بارزة في هذا العصر[2] ،بحيث لا توجد مؤسسة تعليمية أو غير تعليمية إلا و لها اتصال و ارتباط بهذه التقنية ، بل و حتى على مستوى الأفراد أصبحت المعلوماتية محل اهتمام من طرف المتخصصون و غير المتخصصون ، و المنشآت التجارية و غير التجارية [3] .

لكن و رغم الفوائد العديدة التي لا تحصى للمعلوماتية كوسيلة للنهوض و الرقي و التقدم، إلا أنه لا يمكن إنكار سلبيات هذه الأخيرة و الناجمة عن استخدامها لارتكاب الجرائم من لدن المجرمون المعلوماتيون[4].

إذ صار الحديث اليوم عن نوع جديد من الإجرام المستحدث و المتجسد في الجريمة المعلوماتية [5] ، و لأن المشرع الجزائري لم يعرف هذه الأخيرة كان لزاما الاستعانة بالتعريف الفقهي أين

---

[1]- الثقفي نايف عبد الكريم ، الجهود الدولية في مكافحة الاتجار بالبشر عبر شبكة المعلوماتية، مذكرة ماجستير، الأكاديمية العربية للعلوم و التكنولوجيا و النقل البحري ، معهد النقل الدولي و اللوجستيات ، القاهرة ، 2000، ص.08.

[2]- محمد أحمد عبد المحسن بدوي ، الجرائم المعلوماتية ، مقال منشور بمجلة الأمن و الحياة ، الصادرة عن أكاديمية نايف للعلوم الأمنية ، العدد. 335، السعودية ، 2010 ، ص.77.

[3] - نصر محمد عوض القطري،الإشكاليات القانونية لحماية سلامة المعلومات – دراسة تطبيقية على الحماية الجنائية من الاتلاف المعلوماتي ، مجلة الفكر الشرطي ، العدد. 93 ، ابريل 2015 ، ص.167.

[4] - الطحاوي ملك محمد ، الجرائم المعلوماتية أسبابها و مستقبلها،مقال منشور بمجلة كلية الآداب ، جامعة أسيوط، مصر، ع. 28 ، أكتوبر 2008، ص.374.

[5] - رضا عبد الحكيم إسماعيل،حماية حقوق التأليف و النشر الحاسوبي وتقنية الأمن المعلوماتي،مقال منشور بمجلة الشؤون الاجتماعية ، العدد. 91، 2006، ص.30.

أجمع الفقهاء على أن الجريمة المعلوماتية هي كل سلوك إيجابي أو سلبي تقدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة من أجل تنفيذ فعل إجرامي .[1]

و تأخذ الجريمة المعلوماتية عدة صور فقد يكون الهدف من إرتكابها الاعتداء على العرض والشرف و من قبيل ذلك جريمة التحرش الجنسي الإلكتروني ، و الاغتصاب الإلكتروني ، وقد يكون الهدف منها الاعتداء على المحررات الإلكترونية الرسمية من خلال تزويرها ، و قد يكون الهدف منها الاعتداء على ضوابط التسويق و خرقها و من ذلك جريمة التقليد المعلوماتي ، كما قد يكون الهدف منها الإضرار المباشر بالاقتصاد و الاعتداء عليه من خلال تحقيق أرباح طائلة عن طريق استنزاف الاقتصاد .

إذ، و تشير التقديرات إلى أن الاقتصاد الرقمي العالمي يولد سنويا نحو ثلاثة تريليونات دولار ، وهذا الرقم مرشح للزيادة ، إذ تمس الجريمة المعلوماتية من 15 إلى 20 بالمائة من حجم الاقتصاد العالمي الرقمي.

و يتوقع المتخصصون أن تصل تكلفة التهديدات و الجرائم الإلكترونية على مستوى العالم إلى 6 تريليونات دولار عام 2001، فقد وصلت تكلفة التزوير و القرصنة إلى 1.77 تريليونات عام 2015 ، أي ما يمثل نسبة 10 % من حجم التجارة العالمية على النحو المحدد من طرف المنتدى الإقتصادي العالمي ، و بذلك فالقطاعات الخدماتية هي الأكثر عرضة للجرائم المعلوماتية و الأكثر تضرر بنسبة 46%[2].

و إنطلاقا مما سبق يعد موضوع الجريمة المعلوماتية الماسة بالاقتصاد من المواضيع المستحدثة والتي تمثل انفتاح القانون الجنائي على آفاق جديدة تقتضي أن تواجه السياسة الجنائية للمشرع التطورات الراهنة ، سواء بالنص على صور إجرامية جديدة تؤطر الأفعال أو تطويع نطاق تطبيق النصوص العقابية النافذة، أو فرض عقوبات جنائية ، أو النص على تدبير احترازية تساهم في مواجهتها . كما تأتي أهمية الدراسة من تزايد حجم المعلومات المنتشرة على الإنترنيت ، و تصاعد قيمتها بوصفها مصدرا اقتصاديا ، و سياسيا و عسكريا ، مما يشجع قراصنة المعلومات على اختراق دوائرها الأمنية، و أنظمة حمايتها .

---

[1] - معاشي سميرة ،الجريمة المعلوماتية، مقال منشور بمجلة المفكر، كلية الحقوق و العلوم السياسة ، العدد16،جامعة بسكرة ، ص.414.

[2] - نبيلة لعريد، دراسة تحليلية حول الآثار الإقتصادية و المالية الدولية الناتجة عن جرائم نظم المعلومات، المجلد.06، العدد .11، المجلة الجزائرية للاقتصاد و المالية ، ص.193.

و من ثم يصبو هذا البحث لإبراز انعكاسات الثورة المعلوماتية على عملية الاقتصاد الوطني، مع الوقوف على مختلف صور الجريمة الإقتصادية الرقمية .

و بناءا على ما سبق فإن الإشكالية التي تدور حولها الدراسة تتجلى في ما يلي: ما المقصود بالإجرام المعلوماتي الإقتصادي ؟ و إلى أي مدى تصل آثاره على الاقتصاد ؟ .

و للإجابة عن هذه الإشكالية سيتم الوقوف على الإطار العام للجريمة المعلوماتية الماسة بالاقتصاد (المحور الأول) ، ناهيك على تبيان صورها (المحور الثاني) ، من أجل الوقوف على انعكاساتها على الاقتصاد الوطني (المحور الثالث) .

المحور الأول : الإطار العام للجريمة المعلوماتية الماسة بالاقتصاد :

للجريمة المعلوماتية أثر كبير على التنمية الإقتصادية ، وعلى الاقتصاد العالمي فهي تمثل حصة الأسد في حجم الأضرار الماسة بالاقتصاد بالمقارنة مع الأضرار الأخرى ، ناهيك عن تلك الخسائر التي يتكبدها الاقتصاد العالمي من جراء جرائم التسويق الإلكتروني[1]، و بالتحديد من جرائم الغش الإلكتروني و كذلك تجارة المخدرات ، و ذلك من منطلق أن الجريمة المعلوماتية في نظر المجرم الإقتصادي تمثل مجالا للنصب و تحصيل الأموال الطائلة مع تكلفة منخفضة .

إن دراسة الإطار العام للجريمة المعلوماتية الماسة بالاقتصاد الرقمي تتطلب بالضرورة الوقوف على مفهوم المجرم الإقتصادي في البيئة الافتراضية (أولا)، و من ثم تحديد المقصود الإجرام الإقتصادي الرقمي (ثانيا)، مع الوقوف على أهم العوامل المسهلة للإجرام الإقتصادي في البيئة الرقمية (ثالثا) ، ناهيك عن العلاقة بين الإجرام الإقتصادي و الإجرام المعلوماتي.

أولا : تعريف المجرم الإقتصادي في البيئة الافتراضية

يناط بالمجرم الإقتصادي في البيئة الرقمية هو ذلك الشخص هو كل شخص يرتكب سلوك إيجابي أو سلبي يصبو لتحقيق أرباح من خلال الإضرار بالاقتصاد ، و لعل أهم ما يميز المجرم الإقتصادي في البيئة الرقمية هو كونه خبير بالمسائل المعلوماتية ، و له القدرة على التدمير الهادئ و التلاعب بالمعلومات و البيانات ، و ممارسة الإجرام دون عنف و ضد أي قطاع ، و على ذلك سلط عليه القانون مسؤولية جنائية بوصفه فاعل أصلي بالجريمة أو شريك.[2]

- معاشي سميرة، المرجع السابق، 410.[1]

[2] - سالم محمد علي ، الجريمة المعلوماتية ، مقال منشور بمجلة جامعة بابل ، عدد خاص ، 2007/ ص.39.

و قد يكون المجرم الإقتصادي في البيئة الرقمية في كثير من الأحيان من مجرمي الياقات البيضاء، فقد يكوم شخص يمتع بمنصب رفيع ، و من الكفاءات العالية و يمتع بالذكاء و القدرة على التكيف الاجتماعي .

و اتجه الباحثون إلى الإقرار بأفضل تصنيف لمجرمي التقنية ، و هو التصنيف القائم على أساس غرض الاعتداء ، و من أفضل التصنيفات للمجرم المعلوماتي هو الذي أورده بول سارجر وغيره هي ما يلي :

- **المخترقون** ، و يحدد في إطار هذه الفئة نوعين من المحترفون أو المتطفلون، و هم الهاكرز والكراكرز ، و ترى فئة الهاكرز في اختراق الأنظمة المعلوماتية تحد لقدراتهم الذاتية ، فهذه الفئة تتكون من هواة الحاسوب الذين يقومون بأعمالهم لمجرد إظهار أنهم قادرون على اقتحام المواقع الأمنية و سرقة المعلومات و الاحتيال المعلوماتي ، و التجسس المعلوماتي[1]، أو لمجرد ترك بصماتهم التي تثبت وصولهم إلى تلك المواقع ، كما أن هذه الفئة تدعي أنه لا توجد لديهم دوافع جرمية بل فقط الفضول هو محركهم و دافعهم، و إظهار جنون العظمة[2] ، و عموما الهاكرز هو شخص لا تتوافر لديه دوافع حاقدة أو جرمية ، بل فقط إثبات الذات .

يضف إلى ما سبق هذه الفئة تشمل عادة أشخاص يشغلون مناصب محل ثقة و لديهم الكفاءة الخاصة و المعرفة و المهارة المطلوبة في مجال المعلوماتية[3] .

بينما الكراكرز أو المقتحم هو شخص يقوم بالتسلل إلى نظام الحاسوب للإطلاع على المعلومات المخزنة فيه ، أو إلحاق الضرر أو العبث فيها أو سرقتها ، و تم استعمال هذا المفهوم الجديد عام 1985 ، و السمة المميزة للمقتحمين هي تبادلهم للمعلومات فيما بينهم .

- **المحترفون** :إن هذه الطائفة هي أخطر مجرمي الكمبيوتر و الإنترنيت ، إذ يهدف اعتداءاتهم بالأساس إلى الكسب المادي لفائدتهم ، أو لفائدة الجهات التي كلفتهم و سخرتهم لارتكاب جريمة الحاسوب.

---

[1] - عبد الحكيم مولاي إبراهيم ، الجرائم الإلكترونية ، مقال منشور بمجلة الحقوق و العلوم الإنسانية ، جامعة الجلفة ، العدد . 23، الجلفة ، 2015، ص.33.

[2] - محمد ساسي ، الغش المعلوماتي ، مقال منشور بمجلة الأمن و الحياة ، الصادرة عن أكاديمية نايف للعلوم الأمنية ، العدد. 2005، ص.280.

[3]- نهلا عبد القادر المومني ، الجرائم المعلوماتية ، الطبعة .01، دار الثقافة ، عمان ، 2010 ،ص.36.

- **الحاقدون** :هذه الفئة لا تتوافر على أهداف و أغراض للجريمة المتوافرة لدى الفئتين السابقتين، فهم لا يسعون إلى إثبات المقدرات التقنية و لا يسعون لمكاسب مادية ، إنما تحرك أنشطتهم الرغبة بالانتقام و الثأر كأثر لتصرف صاحب العمل معهم ، أو لتصرف المنشاة معهم عندما لا يكونون موظفون فيها ، و لهذا فهم ينقسمون إما إلى مستخدمين للنظام بصفتهم موظفين أو مشتركين ، أو على علاقة بالنظام محل الجريمة،و إلى غرباء عن النظام تتوافر لديهم أساليب الانتقام من المنشأة .

فهي فئة لا تفتخر بنشاطها و تعمد على إخفاءه ، و أعمارهم تتباين، و ليس هناك ضوابط مرتبطة بالسن ، و تعمل هذه الفئة عن طريق تعطيل النظام أو الموقع المستهدف متى تعلق الأمر بموقع أو نشر البرامج و الفيروسات الضارة ، و تخريب و إتلاف الأنظمة أو بعض المعطيات .

و بناءا على ما سبق يلاحظ أن المجرم الإقتصادي في البيئة الرقمية ينتمي إلى الفئة الثانية أي فئة المحترفون .

ثانيا : تعريف الإجرام الإقتصادي الرقمي

يعرف الإجرام الإقتصادي في البيئة الرقمية على أنه جملة المخالفات المرتكبة من طرف أشخاص ذوي مستوى سوسيو إجتماعي و إقتصادي عال ، و يستخدمون البيئة الرقمية بهدف الإضرار بالاقتصاد الرقمي من خلال إتيان جملة من السلوكيات الإجرامية .

و من ثم فالإجرام الإقتصادي و المالي الرقمي هو جملة المخالفات التي تصبو إلى تحقيق أرباح على حساب الاقتصاد من طرف أشخاص لهم حنكة و دراية بالإجرام المعلوماتي ، عن طريق استغلال التقدم التكنولوجي و العولمة الإقتصادية ، و حرية المبادلات دون مراعاة القوانين ، وبطرق و أساليب غير شرعية بهدف تحقيق أرباح تلحق أضرار بالنظم الإقتصادية العالمية [1].

و من ثم تعرف الجريمة الإقتصادية المرتكبة في البيئة الرقمية على أنها كل عمل أو امتناع عن عمل يخالف التشريع الإقتصادي ، و بموجبه يصبو مرتكب الجريمة لتحقيق أرباح عبر البيئة الرقمية مساسا بالاقتصاد الرقمي .

أو هي كل سلوك إيجابي أو سلبي يرمي بموجبه المجرم المعلوماتي إلى تحصيل عائد مادي ، وتحقيق أرباح من جراء إرتكاب جريمة تمس بالاقتصاد الوطني [2].

[1] نبيلة لعريد، المرجع السابق ، ص .193.

[2] - سفيان بوقطاية ، كريمة حاجي ، أسباب و تداعيات تصاعد الجريمة الإقتصادية في الدولة العربية،مجلة الدراسات الإقتصادية ، ع.02، ماي 2018 ، ص.144.

ثالثا :عوامل الإجرام المعلوماتي الماس بالاقتصاد:

هناك عدة عوامل تجتمع لتوليد و تسهيل الإجرام المعلوماتي الماس بالاقتصاد و التي نجملها في ما يلي :

- ضعف بنية شبكة المعلوماتية و قابليتها للاختراق لإنشاء شبكة معلومات مصممة في الأصل بشكل مفتوح دون قيد ، أو حواجز أمنية عليها رغبة في التوسع و تسهيل دخول المستخدمين، إذ تحتوي الأنظمة الإلكترونية و الشبكات المعلوماتية على ثغرات معلوماتية يمكن للمنظمات الإجرامية استغلالها لإضرار بالاقتصاد الوطني .

- غياب الحدود الجغرافية و تدني مستوى المخاطرة ، إذ أن غياب الحدود المكانية في الشبكة المعلوماتية إضافة إلى عدم وضوح الهوية الرقمية للمستخدم المستوطن في بيئته المفتوحة ، يعد فرصة مناسبة للمجرم المعلوماتي الإقتصادي ، إذ يمكنه تقديم نفسه بالصفة و الهوية التي يرغب فيها ، و يمكنه الاختفاء تحت غطاء شخصية وهمية ، و يشن هجوم إلكتروني و هو مسترخ في سريره ، دون أية مخاطرة مباشرة ، و بعيدا عن أعين الآخرين، بل و أكثر من ذلك أصبح بمقدور شاب لم يتجاوز20 سنة أن يتسبب خسائر اقتصادية ضخمة ، بل و شن هجوم على منظمات حكومية والقضاء على استقرار دولة بأكملها ، و إدخالها في حالة طوارئ[1] .

- سهولة الاستخدام و قلة التكلفة ،إن تسمية العولمة لشبكة المعلومات تجلى في كونها وسيلة سهلة الاستخدام دون وقت أو جهد ، فهي إذن فرصة استغلها المجرم المعلوماتي لتحقيق أهداف غير مشروعة دون حاجة لمصادر تمويل ضخم ، و على ذلك فإن شن هجوم و إرتكاب جريمة لا يتطلب أكثر من حاسوب متصل بالشبكة المعلوماتية و مزود بالبرامج اللازمة.

رابعا : العلاقة بين الإجرام الإقتصادي و الإجرام المعلوماتي :

هناك علاقة وطيدة بين الإجرام المالي و الإجرام المعلوماتي ، إذ أن جرائم نظام المعلومات هي جرائم اقتصادية على النحو الذي أقره مؤتمر الأمم المتحدة المنعقد بالقاهرة بموجب البند الرابع و تم إدراجه ضمن جدول الأعمال الخاص بمكافحة الجريمة الإقتصادية و الجريمة المنظمة ، أين اعتبر التقنية وسيلة لارتكاب الجريمة الإقتصادية و لاسيما في ظل الإقبال المتزايد على استخدام

[1] - خالد ممدوح العزي ، الجرائم المالية الإلكترونية ، الجرائم المصرفية نموذجا ، مداخلة مقدمة في فعاليات المؤتمر الدولي الرابع عشر حول الجرائم الإلكترونية ، منشورة بسلسلة أعمال الملتقى ، طرابلس ، 24-25 مارس 2017.

تكنولوجيا المعلومات في تنفيذ الصفقات التجارية غير المشروعة بهدف النصب أو الاحتيال ، ولاسيما و أن المجرم الإقتصادي هو شخص يمتع بالحنكة التي تأهله لإخفاء الأدلة الرقمية .

بالإضافة إلى ما سبق إن الجرائم الإقتصادية تتنوع بتنوع النظام الإقتصادي السائد ، إذ رافق النظام الاشتراكي جريمة التهرب الضريبي و الغش الجمركي ، و الجريمة المصرفية ، في حين أنه عندما يتعلق الأمر بالنظام الرأسمالي فإنها تأخذ صورة أخرى و لاسيما في ظل انتشار الإنترنيت، إذ ساهمت الإنترنيت في عصرنة الجريمة و آليات ارتكابها و ظهرت ما يسمى بالجريمة المعلوماتية. و بذلك فالإجرام المعلوماتي يمثل تحديا جديدا في المجال الإقتصادي ، إذ أن البيئة الرقمية سهلت على المجرم الاعتداء على الاقتصاد ، فهي بذلك حلقة وصل بين المجرم المعلوماتي و الاقتصاد الرقمي ، كما ساهمت البيئة الرقمية في تدويل الإجرام الإقتصادي ، من منطلق أن الإجرام الإقتصادي الرقمي لا يمس باقتصاد دولة واحدة بل يتعدى لأكثر من ذلك .

المحور الثاني : صور الجريمة المعلوماتية الماسة بالاقتصاد الرقمي :

علمنا التاريخ الاقتصادي دوما أنه مهما كانت طبيعة النظام الاقتصادي للدولة و مهما كانت العقيدة السياسية و الاجتماعية لهذا النظام و حتى تلك المبنية على مبدأ " الحرية الاقتصادية الفردية "، أنه من الضروري أن تفرض الدولة إجراءات مناسبة من أجل تنظيم اقتصادها وتوجيهه[1] و فرض كل القيود من أجل حسن حمايته من الجشع و العبث ...

إذ تشكل الجرائم الاقتصادية[2] و الظواهر الإنحرافية تهديدا للسياسة الاقتصادية ، مما يؤدي إلى إلحاق ضرر كبير بالأمن العام ، و السلامة العامة ، و مصالح المجتمع عموما .

---

[1]- عبو السراج ، مكافحة الجرائم الإقتصادية و الظواهر الإنحرافية و الوقاية منها ، ورقة عمل منشورة بمؤلف الجرائم الاقتصادية و أساليب مواجهتها ، الصادر عن أكادمية نايف العربية للعلوم الأمنية ، الطبعة.01 ،دار حامد ، عمان ، 2014 ، الصفحة .39.

[2] - الجريمة الإقتصادية هي كل فعل أو إمتناع له مظهر خارجي يخل بالنظام الإقتصادي للدولة ،و بأهدافه وبالسياسة الإقتصادية للدولة ، يحظره القانون و يفرض له عقابا، يرتكب من طرف شخصا أهلا للمسائلة الجنائية و لمزيد من التفاصيل حول المفهوم أنظر ، محمد محي الدين عوض ، أهم الظواهر الإنحرافية و الإجرامية ، ورقة عمل منشورة بمؤلف الجرائم الإقتصادية و أساليب مواجهتها ،الصادر عن أكادمية نايف العربية للعلوم الأمنية ، الطبعة.01 ، دار حامد ، عمان ، 2014 ، الصفحة .39.

هذا و قد تزايد خطر الجرائم الاقتصادية في كثير من البلدان مما أدى إلى إصابتها بأضرار اجتماعية و اقتصادية فادحة ، إذ لم تعد الجريمة الاقتصادية مقيدة بحدود دولة واحدة بل عبرت كل الحدود و ارتدت آثارها إلى دول أخرى.[1]

فقد تقع الجريمة الاقتصادية في دولة معينة و يتم تنفيذها في دولة أخرى أو في عدة دول ، و قد ينتمي مرتكبوها إلى عدة جنسيات ، مما حذا بالعديد من الدول للتعاون في مكافحة الإجرام الاقتصادي ، باعتبار أن هذا النوع من الإجرام يمس بالمصالح الوطنية للدول بالإضافة إلى المصالح الدولية[2] .

و بالتالي للجريمة المعلوماتية الماسة بالاقتصاد الرقمي عدة صور فقد تأخذ صورة جريمة تبيض الأموال الرقمي (أولا) ، أو جرائم نظم المعلومات (ثانيا) ، أو جرائم مالية (ثالثا) .

أولا : جريمة تبيض الأموال في البيئة الرقمية :

يناط بجريمة تبيض الأموال في البيئة الرقمية جملة السلوكيات التي يصبو من خلالها المجرم الإقتصادي لاستعمال الرقمنة بهدف تبيض الأموال القذرة و السوداء ، و لعل الوسيلة المثلى هي تلك الحالة التي بموجبها يقوم صاحب الأموال القذرة باستثمار أمواله عبر البيئة الرقمية من خلال القيام بمعاملات رقمية ، من خلال البيع و الاستثمار الرقمي بهدف توظيف تلك الأموال و إخفاء عدم مشروعيتها .

و قد نظم المشرع الجزائري جريمة تبيض الأموال و بين أحكامها في القسم السادس من الفصل الثالث من الباب الثاني من الكتاب الثالث من قانون العقوبات و ذلك بموجب المواد من 389 مكرر إلى 389 مكرر 07 ، هذه المواد التي تشكل الركن الشرعي للجريمة .

إذ تنص المادة 389 مكرر من قانون العقوبات على أنه " يعتبر تبييضا للأموال :

أ- تحويل الممتلكات أو نقلها مع علم الفاعل أنها عائدات إجرامية، بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتي منها هذه الممتلكات على الإفلات من الآثار القانونية لفعلته .

---

[1] - حسين محمد سليمان،مكافحة الجرائم الإقتصادية و الظواهر الإنحرافية والوقاية منها،ورقة عمل منشورة بمؤلف الجرائم الإقتصادية و أساليب مواجهتها ، الصادر عن أكاديمية نايف العربية للعلوم الأمنية ، الطبعة.01، دار حامد ، عمان ، 2014 ، الصفحة. 213.

[2] - مصطفى التونسي ، مكافحة الجرائم الإقتصادية و الظواهر الإنحرافية و الوقاية منها،ورقة عمل بمؤلف الجرائم الإقتصادية و أساليب مواجهتها ، الصادر عن أكاديمية نايف العربية للعلوم الأمنية ، الطبعة.01 ،دار حامد ، عمان ، 2014 ، الصفحة. 301. منشورة

ب- إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها ، مع علم الفاعل أنها عائدات إجرامية .

ج- اكتساب الممتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك وقت تلقيها ، أنها تشكل عائدات إجرامية .

د- المشاركة في ارتكاب أي جريمة من الجرائم المقررة وفقا لهذه المادة ، أو التواطؤ أو التآمر على ارتكابها و محاولة ارتكابها و المساعدة و التحريض على ذلك و تسهيله و إسداء المشورة بشأنه".

مع الإشارة أن المشرع الجزائري نص على جريمة تبيض الأموال في البيئة التقليدية دون الرقمية و هي نقطة تحسب على المشرع الجزائري ، إذ و من صور جريمة تبيض الأموال الرقمية نجد تلك الحالة التي يحصل فيها مبيض الأموال أو المجرم الإقتصادي على عدة بطاقات إئتمان من عدة بنوك من أجل تهريب الأموال أو العائدات الإجرامية من بنك لآخر و من دولة لأخرى .

ثانيا: جرائم نظم المعلوماتية الماسة بالاقتصاد:

باعتبار أن الجريمة المعلوماتية قد تستهدف المعلومات أو برامج الحاسوب أو الأموال ، فقد يكون الهدف منها الدخول غير المصرح به إلى أنظمة الحاسوب و الشبكات و بالإستلاء على المعلومات أو إتلافها عبر تقنية الفيروسات و غيرها من وسائل التدمير المعلوماتي ، و جرائم قرصنة البرمجيات و الاعتداء على حقوق المكية الفكرية .

و من ثم فإن نظم المعلومات تضر لا محالة بالاقتصاد فهي جرائم تكلف الدولة أعباء بهدف التحقيق و التحري و ضبط مرتكبيها .

ثالثا: الجرائم المعلوماتية الماسة بالقطاع المالي

عادة ما تنقسم الجرائم المعلوماتية إلى قسمين الأولى جرائم يكون الحاسب فيها هدف للجريمة، ومن أمثلتها القيام بفتح حساب في البنك من قبل موظف البنك ، و تحويل مبلغ معين من حسابات المودعين ، حيث لا يهتم المودع بهذا المبلغ نظرا لقتله ، أو استخدام كلمة السر للمسئولين من الجامعات أو الشركات الكبرى،بينما تجلى الثانية في الجرائم التي يكون فيها الحاسب أداة في الجريمة في هذا النوع من الجرائم باستخدام غير قانوني للحاسب ، أو استخدامه قانونيا و لكن لأغراض غير مسموح بها ، بما في ذلك الدخول غير القانوني على نظام الحسابات الخاصة .

و من أمثلة العمليات المالية الرقية غير القانونية أيضا نجد الدخول على حسابات العملاء، وتحويلها إلى حساب شخص أو سرقتها ، بالإضافة إلى سرقة الممتلكات عن طريق الحاسب ، أو نقل ملكيتها بطريقة غير شرعية.

إذ نص عليها المشرع الجزائري بموجب المادة رقم 394 مكرر من القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، المعدل لقانون العقوبات على الدخول غير المشروع أو تغيير المعطيات أو تخزين نظام المعالجة الآلية للمعطيات ، و يستوي في ذلك أن يتم إرتكاب الجريمة أو أن يتوقف الأمر عند مرحلة الشروع [1].

كما أورد المشرع الجزائري بموجب المادة 384 مكرر 05 حكم خاص متعلق بالمشاركة بالجريمة ، إذ يعاقب بالعقوبة المقررة للجريمة ذاتها كل من شارك في مجموعة أو اتفاقات تعقد بهدف الإعداد لجريمة أو أكثر من الجرائم المعلوماتية ، كما يعاقب على الشروع بذات العقوبة المقررة للجنحة ، وتطبق عقوبة المصادرة للأجهزة و البرامج و كل الوسائل المستحدثة محلا للجريمة ، مع إمكانية الحجز على المحل متى كان صاحبه على علم بالجريمة .

و عندما يتعلق الأمر بالشخص المعنوي فإنه يعاقب مرتكب الجريمة المعلوماتية الماسة بالاقتصاد بعقوبة تصل إلى خمس مرات تلك العقوبة المقررة للشخص الطبيعي على النحو المنصوص عليه بموجب المادة 394 مكرر 04.

المحور الثالث :الآثار الإقتصادية للجريمة المعلوماتية و انعكاساتها في ظل صعوبة الإثبات

للجريمة المعلوماتية الماسة بالاقتصاد الرقمي عدة آثار يتوجب الوقوف عليها (أولا) ، ناهيك عن ضرورة الوقوف على معوقات إثبات الجريمة المعلوماتية الماسة بالاقتصاد الرقمي (ثانيا) .

أولا : الآثار الناجمة عن الجريمة المعلوماتية و انعكاساتها على الاقتصاد

تتجلى أهم الآثار الناجمة عن الجريمة المعلوماتية الماسة بالاقتصاد في ما يلي :

1- المساس بالاستقرار المالي و الإقتصادي:

إن الاستقرار المالي و الإقتصادي يعد مطلبا هاما في أي دولة لضمان الاستقرار ، و تعد الجرائم الإقتصادية في البيئة الرقمية من أهم عوامل عدم الاستقرار ، فإن تعلق الأمر بالمجرم الإقتصادي الذي يستعمل البيئة الرقمنة لتبيض أمواله و توظيفها في مشاريع ، فإنه لا يتوانى في تصفية المشاريع بمجرد تحقيق أهدافه ، مما يمس باستقرار الاقتصاد.

2- الخسائر المالية المنجرة على الجريمة المعلوماتية

[1]- الأمر 156/66 ، المؤرخ في 08 جوان 1966 ، المتضمن قانون العقوبات المعدل و المتمم .

لاشك أنه واكب التحول الذي عرفه الاقتصاد العالمي تحول الاقتصاد من اقتصاد تقليدي إلى اقتصاد رقمي تحول المعاملات التجارية و المالية إلى طبيعة إلكترونية ، و هو ما زاد من خطورة الجريمة المعلوماتية و نجم عنه خسائر كبيرة يتكبدها العالم [1].

و بذلك يمكن القول أن رقمنة التعاملات التجارية التي يقوم بها أشخاص طبيعيون و شركات التسويق نجم عنها ارتفاع معدل الإجرام المعلوماتي و بالنتيجة لذلك استنزاف الاقتصاد.

إذ تبين من خلال الإحصائيات أن الاقتصاد العالمي يتضرر من جراء الجريمة المعلوماتية سنويا أي ما يعادل تريليون دولار سنويا .

و الإشكال ليس فقط في ارتفاع حجم الخسائر المالية ، بل إن الأمر أخطر من ذلك ، إذ أن تزايد الإقبال على المعلوماتية الذي يزيد يوميا جعل حجم الخسائر غير ثابت ، فقد أصبحت الخسائر الناجمة عن الجريمة المعلوماتية ضريبة لا مفر منها [2].

ناهيك عن سرقة المعلومات التجارية الحساسة ، و كذلك الأثر السلبي للجريمة المعلوماتية على أداء الشركات التجارية و حركة التجارة العالمية ، ناهيك عن القدرة التنافسية و الابتكار.

3-إحداث العجز في ميزان المدفوعات

تؤدي الجريمة المعلوماتية ذات الطابع الإقتصادي إلى إحداث عجز في المدفوعات و لاسيما في حالة استعمال الرقنة بهدف التهرب من دفع الضرائب ، كما تساهم الجريمة المعلوماتية في زيادة الإنفاق العام بهدف مواجهتها .

4- الإضرار بالنشاط المصرفي :

إذ تؤدي الجريمة المعلوماتية إلى إفساد نشاط البنوك عن طريق التعامل بالعملات الرقمية المزورة، و بطاقات الإئتمان المزورة ، ناهيك عن كون الجريمة المعلوماتية تسبب انهيار في سوق القيم المنقولة ، في حالة استثمار الأموال الإجرامية المحصلة عن طريق البيئة الرقمية في سوق القيم المنقولة ، من خلال شراء أوراق مالية من عائدات إجرامية مما يحدث خلل في توازن سوق القيم المنقولة مما يؤدي إلى انهيار سوق القيم المنقولة .

5- ارتفاع معدل التضخم :

---

[1] - صراح كريمة ، دقيش جمال ، الأبعاد التسويقية ، مجلة الدراسات التسويقية ، مجلد رقم 02 ، ع.01، جانفي2018 ، ص.44.

[2] - صراح كريمة ، دقيش جمال ، المرجع السابق ، ص.46.

إن الجريمة المعلوماتية قد تكون مؤشر لحدوث تضخم أو زيادة معدلة في حالة كان موجود من قبل ، و يتحقق ذلك في تلك الحالة التي تطرح أموال غير مشروعة محصلة عن طريق البيئة الرقمية بغض النظر عن نوع الجريمة قصد توظيفها و استثمارها مما يؤدي إلى الزيادة في أسعار السلع والخدمات و بالنتيجة ارتفاع قيمتها .

6- انخفاض معدل الاستثمار و الادخار

غالبا ما يقوم المجرم الإقتصادي الذي حصل على أموال عن طريقة البيئة الرقمية بإخراج الأموال التي جمعها من إقليم الدولة التي تم استنزاف اقتصادها إلى إقليم دولة أخرى ، و ذلك بهدف إخفاء الشبهة و هو ما يؤدي إلى انخفاض معدل الاستثمار بسبب نقص التمويل ، ناهيك عن انخفاض معدل الاستثمار الذي يعد مؤشرا على سلامة اقتصاد الدولة.[1]

كما ساهمت المعلوماتية في خلق سرعة كبيرة لحركة رؤوس الأموال ، و سهلت الربط بين الأسواق العالمية في إطار نظام تبادلي ، و حفزت المعلوماتية الشركات العابرة للحدود ، مما زاد في حجم التفاعل بين المتعاملين الاقتصاديين و ساهم في تفشي التهريب .

ثانيا :معوقات إثبات الجريمة المعلوماتية الماسة بالاقتصاد

هناك عدة معوقات تحول دون إثبات الجريمة المعلوماتية الماسة بالاقتصاد الرقمي التي يمكن اختصارها في ما يلي :

أ- عدم وجود آثار مادية للجريمة

إن خصوصية الجريمة المعلوماتية الماسة بالاقتصاد جعلتها تنفرد بذاتية مقارنة بباقي الجرائم ، الأمر الذي جعل عملية الكشف عنها من طرف السلطات جد صعبة و لاسيما مع افتقارها للدليل الرقمي[2]، و يبقى أغلبها مجهول ، يضف إلى ذلك إن مرتكب الجريمة يبذل قصارى جهده لعدم ترك أي أثر مادي ، ناهيك عن عدم تمكن الكل من التحكم في المعلوماتية ، و لا شك أن جهل المعلوماتية ساعد المجرم الإقتصادي في إرتكاب الجريمة[3].

---

[1]- بسام أحمد الزلمي ، عبود السراج ، دور النقود الإلكترونية في عمليات غسيل الأموال، مقال منشور مجلة العلوم الإقتصادية و القانونية ، جامعة دمشق ، المجلد رقم. 36، العدد .01، 2010 ، ص.354.

[2] - فيصل فهد ، انتهاك الخصوصية ، مقال منشور بمجلة الأمن و الحياة ، الصادرة عن أكاديمية نايف للعلوم الأمنية ،، العدد . 378 ،السعودية ، أكتوبر 2013، ص.03.

- بن بادرة عبد الحليم ، إجراءات البحث والتحري عن الجريمة المعلوماتية – الخصوصية والإشكالات ،مجلة [3] الحقوق والعلوم الإنسانية ، العدد. 23 ، ص.150.

ب- اتسام الجريمة المعلوماتية الماسة بالاقتصاد بكونها جريمة عابرة للحدود :

إن العولمة و المعلوماتية جعلت العالم قرية واحدة ، إذ و رغم إيجابيات العولمة إلا أن المجرمون استغلوا هذه الأخيرة من أجل تسهيل إرتكاب الجرائم ، أين تعدى الإجرام حدود الدولة الواحدة، و صار بإمكان المجرم اختراق حساب أو موقع أو حساب بنك معين دولة معينة ، وله تحويل المبالغ و العملات إلى دولة ثالثة ، دون أن يتحرك من مكانه و هو ما يسمى بالإجرام عن بعد، و بدون استعمال العنف بل و هو مستلق بسريره ، إذ صار بغير حاجة لكسر الأقفال و لا إخفاء البصمات أو تحويل العائدات الإجرامية ، بل يكفيه خط إنترنيت و حاسوب حتى يجول و يصول بكافة أنحاء العالم مرتكبا جرائمه الإقتصادية من تزوير بطاقات الإئتمان و احتيال سبيراني...

ج- المعوقات القضائية

تتجلى المعوقات القضائية التي تحول دون إمكانية الكشف عن الجريمة الإقتصادية المرتكبة في البيئة الرقمية في ما يلي :

- نقص الخبرة لدى جهات البحث و التحري و التحقيق بالجريمة المعلوماتية ، أي نقص الخبرة لدى رجال الضبط القضائي و الأمن عموما ، و أجهزة العدالة الجنائية ممثلة في سلطة الاتهام والتحقيق ، و لاشك أن من شأن ذلك الحيلولة دون الكشف عن الجريمة المعلوماتية المرتكبة في البيئة الرقمية [1].

- و من بين المعوقات القضائية ايضا ما يعرف بتنازع الاختصاص القضائي بين العالمية والإقليمية، و لاسيما و أن السلوك المادي للجريمة الإقتصادية قد يكون بإقليم دوله ، و النتيجة الإجرامية بإقليم دولة أخرى .

د- المعوقات المرتبطة بإثبات الجريمة في حد ذاتها :

من بين معوقات الإثبات و المرتبطة بالجريمة في حد ذاته نشير إلى :

- اتخاذ الجناة لتدابير أمنية ، أين يسعى المجرم الإقتصادي لإخفاء الدليل المعلوماتي و تمويهه ، في شكل عطل أو خطأ في نظام التشغيل ، مع إزالة آثار الجريمة عن طريق التلاعب بالبيانات الرقمية أي المكتوبة بروز رقمية ، لا يمكن فهمها إلا من طرف الحاسوب ، مع قيامه بتشفير البيانات مما يجعل مسألة فكها أمر مستحيل ، و من ثم يصعب على جهات التحري الوصول إليها ، ناهيك عن الانتحال الرقمي أين ينتحل المجرم المعلوماتي صفة أخرى غير صفته .

---

[1]- بن بادرة عبد الحليم ، المرجع السابق،ص.151.

- الطبيعة غير المادية للأدلة الإلكترونية التي ارتكبت بها الجريمة الإقتصادية ، إذ عادة ما يكون الدليل بالجريمة التقليدية مرئي إما سلاح ابيض ، أو مادة سامة ، أو محررات مزورة ، غير أنه و عندما يتعلق الأمر بالجريمة المعلوماتية فإن أداة الجريمة هي غير مادية و يصعب الكشف عنها، من منطلق أن قوامها معنوي مرتبط بالمعالجة الآلية للبيانات ، مع إمكانية تدمير الدليل الرقمي في ثوان في عملية التفتيش و دون قصد .

- ضخامة حجم المعلومات و البيانات المتعين فحصها ، إذ متى قامت جهات التحقيق في فإن مصرح الجريمة غير واضح المعالم ، في ظل العالم الافتراضي مما يجعل المعاينة صعبة و لاسيما مع اصطدامه بفكرة المشروعية و حق الفرد بالخصوصية[1] ، و هو أمر شاق نظرا لنقص الإمكانيات المادية والبشرية ، مما يؤدي للخطأ بالتحقيق و تكرار العملية، إذ يمكن للجاني و بسهولة و سرعة القيام بتدمير الدليل الرقمي دون ترك أي أثر، و كل ذلك ينعكس سلبا على الاقتصاد الوطني فتكاليف التحقيق و التحري في خد ذاتها تستنزف الاقتصاد .

الخاتمة

إن الجريمة المعلوماتية تمثل نمط إجرامي جديد فرض نفسه على الواقع العملي، مما دفع بالمشرع الجزائري لسن ترسانة قانونية يطمح بموجبها للموازنة بين مطلبين ،يتجلى أولهما في توفير البيئة الحمائية الكافية لمستخدم الانترنيت من أجل الاستفادة من المعلوماتية و مزاياها التي مكنت من كل مستحيل ، وثانيهما في كبح جماح كل هاو لمجال المعلوماتية و متمكن في الرقمنة ، حتى لا يستغل ذكاءه المعلوماتي في إرتكاب الجرائم عن طريق الانترنيت .

و مهما تعددت صور الجريمة المعلوماتية فإن جل إن لم نقل كل الجرائم المعلوماتية تستهدف الاقتصاد الوطني ، و تحول دون تحقق التنمية الإقتصادية، سواء بطريقة مباشرة عن طريق إرتكاب الجريمة الإقتصادية الرقمية ، أو بطريقة غير مباشرة من خلال ما تتكبده خزينة الدولة من خسائر ناجمة عن المتابعة و التحري و البحث عن الدليل الرقمي .

و بالبحث حول مدى نجاعة المنظومة القانونية الجزائري في تأطير الجريمة المعلوماتية عموما ، والماسة بالاقتصاد خصوصا ، اتضح أنه رغم سعي المشرع الجزائري الدؤوب لخلق بيئة قانونية

---

[1]- زوزو هدى، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري دفاتر السياسة والقانون ، العدد . 11، جامعة قاصدي مرباح ورقلة ، جوان 2014، ص.122.

فعالة تؤطر البيئة الرقمية بكل أبعادها ،إلا أنه تطرح جملة من الثغرات التشريعية التي تحول دون فعالية الحماية القانونية .

بل و أكثر من ذلك إذا كانت جريمة تبيض الأموال الرقمية ، و الجرائم الماسة بالقطاعات المالية تشكل جرائم اقتصادية رقمية ، فإنه تطرح عدة إشكالات تعتري التنظيم القانوني لهذه النوع من الجرائم ، فإن سلمنا بأنها لا تعدوا كونها ترجمة رقمية للجريمة الإقتصادية ، فإن إعمال مبدأ شرعية التجريم و العقاب سيكون عائقا، و الذي بموجبه لا يمكن تجريم فعل ما لم يجرمه القانون وفقا لما نصت عليه المادة الأولى من قانون العقوبات ، و من ثم لا يكفي قياس أحكام الجرائم الإقتصادية على الجرائم الإقتصادية الرقمية.

وربما في الوقت الذي لا تزال المنظومة القانونية الجزائرية بحاجة لإعادة النظر في تنظيم الجريمة المعلوماتية، نجد تشريعات أخرى تتسابق لتجريم الجرائم الناجمة عن الروبوتات، و هذا إن دل على شيء فهو يدل أن التجربة الجزائرية في مجال الجريمة المعلوماتية لا تزال فتية و قاصرة عن مواكبة التطورات التي يطرحها الواقع العملي ، و تحتاج للعصرنة كي تكون أهلا لمواجهة تحديات الواقع.

وانطلاقا من كل ما سبق يمكن القول أنه آن الأوان ليكون التجريم و العقاب ذو حركية ومرونة تماشى و الأبعاد المستقبلية ، باعتبار أن تكنولوجيا المعلومات في تطور سريع ، ناهيك عن ضرورة تضافر الجهود الرسمية و غير الرسمية للحد من مضار الجريمة المعلوماتية .



المحور السادس

خصوصية المتابعة في الجريمة المعلوماتية

الخصوصية الإجرائية للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري.

Procedural specificity of crimes against automated data-handling systems in Algerian legislation

د.جزول صالح أستاذ محاضر " أ "
معهد الحقوق والعلوم السياسية
المركز الجامعي مغنية- الجزائر

مقدمة:

لعل من ابرز الجرائم المعاصرة التي طفت على السطح ،و أصبحت تشكل عائقا في شتى المجالات تلك الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ،و لعل أخطرها وأصعبها تلك الأفعال التي تشكل اعتداء على النظم المعلوماتية وما تخزنه من معلومات خاصة وهامة ،أما خطورتها فتكمن في كونها تمس بالأشخاص والكيانات والمؤسسات، وأما صعوبتها فتكمن من حيث مسرح ارتكابها الذي يختلف عن مسرح الجريمة التقليدية ، والذي لا يحده مكان ولا زمان، وكذا من حيث الأساليب التي يعتمد عليها الجاني لاقترافه هذه الجرائم ولطمس آثارها التي قد تشكل دليلا لإقامة الدعوى ضده.

ومن هنا تكمن أهمية هذه الورقة التي تبحث في مدى مواكبة المشرع الجزائري لمثل هذه الجرائم من حيث أساليب التحري و التحقيق فيها ، وما يجب أن تصاحبها من ضمانات عدم المساس بحقوق الدفاع من جهة ، ومن حيث قدرة و أهلية الجهات القضائية العادية للنظر في مثل هذا النوع من الجرائم من جهة أخرى .

وللإجابة على هذه الإشكالية ارتأينا تقسيم هذه الورقة البحثية إلى محورين وهما:

المحور الأول :ماهية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

أ- مفهوم أنظمة المعالجة الآلية للمعطيات.

ب- صور السلوك الإجرامي الماس بأنظمة المعالجة الآلية للمعطيات.

المحور الثاني : التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والجهة المختصة بالنظر فيها.

أ- التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

ب- الجهة المختصة بالنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

المحور الأول

ماهية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

تعتبر الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات مظهرا من مظاهر الجريمة الإلكترونية[1] التي تستهدف أحد أو كل العناصر التالية :المعلومات ، الأجهزة ،الأشخاص أو الجهات[2]،وهي تنتج عن استخدام المعلوماتية والتقنية الحديثة ،تقع في فضاء افتراضي غير واقعي ،بقصد تحقيق أغراض قد تتعلق بتحصيل عوائد مالية من خلال هذه الجرائم ،وقد تكون بغرض الإضرار المعنوي والتخريب فحسب ، ولهذا حاولت الدول التصدي لمثل هذا النوع من الجرائم بتبني سياسة جنائية خاصة ،سواء قبل ارتكاب الجريمة وقاية منها ، أو بعد ارتكابها تتعلق بالتجريم والعقاب من جهة، وبإجراءات المتابعة والتحقيق والتنفيذ من جهة أخرى[3].

والمشرع الجزائري على غرار غيره من المشرعين حاول مواجهة الجريمة المعلوماتية بمجموعة من الآليات من بينها تجريمه لمجموعة من الأنشطة ،والأفعال التي من شأنها المساس بالبيانات، والمعطيات المعالجة آليا ،وذلك من خلال نصوص المواد 394مكرر ،394 مكررا1 و 394 مكرر2

---

[1]- لم يتفق الفقه الجنائي على تسمية موحدة للجريمة الإلكترونية، إذ يطلق عليها البعض الجريمة الإلكترونية وهناك من يسميها الجريمة المعلوماتية، ويذهب آخرون إلى تسميتها بجرائم إساءة استخدام تكنولوجيا المعلومات والاتصال ويطلق عليها آخرون مسمى جرائم الكمبيوتر والإنترنت.

وتعريف الجريمة الإلكترونية كان محال لاجتهادات الفقهاء، فقد ذهبوا في ذلك مذاهب مختلفة ووضعوا تعريفات شتى وبالتالي فلا نجد تعريفاً محدداً للجريمة الإلكترونية.

وهناك اختلاف بين الباحثين في تعريف الجريمة الإلكترونية، فمنهم من يتناول التعريف من الجانب التقني فنياً ومنهم من يتناوله من الزاوية القانونية. فالذين يتناولونه من الجانب التقني يذهبون إلى القول بأن الجريمة المعلوماتية ما هي إلا "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود".ينظر بالتفصيل بحث الجريمة الإلكترونية ،في المجتمع الخليجي وكيفية مواجهتها ،إعداد مجمع البحوث والدراسات ، أكاديمية السلطان قابوس لعلوم الشرطة في إطار مسابقة جائزة الأمير نايف بن عبد العزيز للبحوث الأمنية لعام 2015م ،نزوى – سلطنة عمان ، 2016م ، ص20.

[2]- عبد الله عبد الكريم عبد الله ، جرائم المعلوماتية والأنترنت ، (الجرائم الإلكترونية) ، دراسة مقارنة ، منشورات الحلبي الحقوقية ، بيروت ، ط1 ، 2007م ، ص18،19.

[3]- هدى حامد قشقوش ،السياسة الجنائية لمواجهة الجريمة المعلوماتية ،دار النهضة العربية ،2012م ، ص 11- 14

وما يليها من قانون العقوبات ،حيث بينت هذه النصوص العناصر المادية للجرائم الماسة بأنظمة المعالجة للمعطيات ،وكذا ركنها المعنوي والظروف المشددة للعقوبات المقررة لها.

أولا : مفهوم أنظمة المعالجة الآلية للمعطيات .

لم يعرف المشرع الجنائي الجريمة الماسة بأنظمة لمعالجة الآلية للمعطيات ، بل ترك ذلك للفقه والقضاء ،وإنما اكتفى فقط بتحديد السلوك المشكل لهذه الجريمة وصورها ، ولاشك أن هذا يرجع لإمكانية التحكم في الجريمة نظرا لتطور وسائل الجريمة المعلوماتية بتطور تقنية المعلومات[1] المتجددة باستمرار .

كما لم يبين أيضا **المشرع الجنائي** المقصود بمصطلح **أنظمة المعالجة الآلية للمعطيات** ، والتي تعتبر شرطا أساسيا في هذه الجرائم ، فمصطلح أنظمة المعالجة الآلية للمعطيات مفهوم تقني وفني يتأثر بما يحصل من تطور في مجال الإعلام الآلي، وتقنية المعلومات والاتصال ، وهو من اختصاص هذا الأخير ،غير أن القانون 09 -04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[2] ،قد عرف بعض العناصر المرتبطة ارتباطا وثيقا به مثل المنظومة المعلوماتية ، وكذا المعطيات المعلوماتية على الرغم من أن هذه المفاهيم لا يلزم به القضاء الجنائي باعتبار أنها لا تطبق في الأصل إلا على مقتضيات القانون 09-04 ، وإن كان القضاء الجنائي بمقدوره تبني تلك المفاهيم من باب الاجتهاد وليس الإلزام .

فقد عرف القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ، **المنظومة المعلوماتية** بأنها " كل نظام منفصل ،أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".[3] وهذا

---

[1]- تعرف المادة 2 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بأنها " أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا".

مرسوم رئاسي 14-252 مؤرخ في 8 سبتمبر 2014 يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة في ديسمبر 2010م،. ج ر بتاريخ سبتمبر 2014 م ، العدد 57.

[2]- القانون 09-04 مؤرخ في 5 أوت 2009 ،يتظم القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ،ج ر ، مؤرخة في 16 أوت 2009م ، العدد 47.

[3]- المادة 2/ ف ب من القانون 09-04.

التعريف يقترب مع مفهوم منظومة الكمبيوتر[1] التي جاءت بها الاتفاقية الأوربية المتعلقة بالجريمة الالكترونية ، المبرمة ببودابست بتاريخ 23-11-2001م . في حين عرف القانون 09-04 ، **المعطيات المعلوماتية** ، " كل عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها "[2].

وفي المقابل أيضا عرّف القانون 18-04 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[3] **المعالجة الآلية** بأنها " تلك العمليات المنجزة كليا أو جزئيا بواسطة طرق آلية مثل تسجيل المعطيات وتطبيق عمليات منطقية و/أو حسابية على هذه المعطيات أو تغييرها أو مسحها أو استخراجها أو نشرها" ،وهذا التعريف يتوافق مع ما جاء به القرار الفرنسي المتعلق بإثراء مصطلحات الإعلام الآلي المؤرخ في 22 ديسمبر 1981[4] حيث عرف **المعالجة الآلية للمعطيات** ،بأنها جميع العمليات التي تتم بوسائل آلية تتعلق بجمع البيانات وتسجيلها ومعالجتها وتعديلها وحفظها وتدميرها وتحريرها وبصفة عامة استغلالها.[5]

أما الفقه الفرنسي فقد عرّف **نظام المعالجة الآلية للمعطيات** بكونه " كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة

[1]- المادة 1/ف أ .

[2]- المادة 2/ ف ج من القانون 09-04.

[3]- المادة 03 / ف5 من القانون 18-04 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ،المؤرخ في 10جوان 2018م ، ج ر مؤرخة في 2018 ، العدد 34. ،

[4] -« Enrichissement du vocabulaire de l'informatique » Arrêté du 22 décembre 1981 . Bulletin des bibliothèques de France (BBF), 1982, n° 6, p. 355-358. Disponible en ligne : <http://bbf.enssib.fr/consulter/bbf-1982-06-0355-009>. ISSN 1292-8399.

[5] -Traitement automatique des données (n. m.) :Ensemble des opérations réalisées par des moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation, la destruction, l'édition de données et d'une façon générale leur exploitation.

الربط والتي يربط بينها مجموعة من العلاقات التي عن طريقها تحقق نتيجة معينة على أن يكون هذا المركب خاضع لنظام الحماية الفنية" [1].

وبناء على مفاهيم هذه العناصر كلها فإن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يشترط لتحققها فضلا عن ركنها المادي والمعنوي ضرورة توافر شرطا أوليا أساسيا ،ألا وهو عنصر نظام المعالجة الآلية للمعطيات ،أي مساس السلوك المجرم سواء كان إيجابيا أو سلبيا بنظام المعالجة الآلية للمعطيات أو بالمعطيات المعلوماتية الموجودة عليه في شكل الصور المحددة قانونا.

ثانيا :صور السلوك الإجرامي الماس بأنظمة المعالجة الآلية للمعطيات.

إن السلوك الإجرامي الذي يشكل مساسا بأنظمة المعالجة الآلية للمعطيات قد يكون سلوكا ايجابيا ،أو سلوكا سلبيا ، ويشترط فيه أن يرتكب عن طريق الغش ، وقد عبرت عنه الاتفاقية العربية الخاصة بمكافحة جرائم التقنية المعلوماتية بأن يكون بدون **وجه حق** والذي يجوز أن يشير إلى السلوك الذي يتم دون سلطة سواء كانت تشريعية ، تنفيذية ، إدارية ،قضائية ، تعاقدية ،أو توافقية.[2] وقد نص المشرع الجزائري على بعض صور السلوك الإجرامي التي تشكل مساسا بأنظمة المعالجة الآلية للمعطيات، وذلك من خلال المواد 394مكرر ، 394 مكررا1 ، 394مكرر2 ق ع ج ،دون النص على ضرورة توافر الحماية التقنية لهذه الأنظمة لاعتبار الفعل جريمة ، وتتمثل صور السلوك في ما يلي :

1- الدخول غير المشروع في منظومة للمعالجة الآلية للمعطيات أو البقاء فيها .

سواء دخل الفاعل أو بقي في كل المنظومة أو في جزء منها ،ولا يستلزم المشرع الجزائري في هذه الصورة ضرورة أن يترتب على الدخول أو البقاء ضرر، بحيث مجرد الدخول يعتبر الفعل جريمة، وكذلك البقاء في المنظومة المعلوماتية بعد الدخول إليها عن طريق الخطأ أو الصدفة ، يعتبر جريمة شرط أن يكون هذا الدخول عمدا وبغير وجه حق ، وقد عبر عليه المشرع الجزائري أنه يكون بطريق الغش.

---

[1]- الحسن اولياس ، الجريمة الالكترونية والحماية القانونية لنظم المعالجة الآلية للمعطيات وحسابات الأشخاص عبر مواقع التواصل الاجتماعي ،نموذجا ، https://www.marocdroit.com/ ، تاريخ الاطلاع على الموقع 31 مارس 2020 ، على الساعة 19.01سا.

[2]- التقرير التفسيري لاتفاقية الجريمة الإلكترونية ، الخاصة بأروبا ،بودابست المؤرخة في 23 نوفبر 2001م ،مجلس اروبا ، سلسلة المعاهدات الأوربية 185.

وقد جرم المشرع مجرد الدخول لما يشكله هذا الفعل من خطورة إذ يعتبر مرحلة أساسية لارتكاب بقية الجرائم المعلوماتية الأخرى ،كما أن المعلومات التي يقع عليها هذا السلوك تكون معلومات على قد من الأهمية كما هو الحال بالمعلومات المتعلقة بالأسرار العسكرية للدولة ، وكذلك البيانات الخاصة بالعملاء في البنوك ،وغير ذلك من المعلومات المهمة ، بل يعتبر الدخول إلى الأنظمة المعلوماتية جريمة حتى ولو كان من باب إثبات القدرات لاختراق الحواجز التقنية لأن ذلك يؤدي إلى التمادي في الاعتداء على الأنظمة المعلوماتية[1]،كما تحقق هذه الصورة مهما كانت صفة الفاعل الذي قام بالدخول أو البقاء في المنظومة المعلوماتية سواء كان من أهل الاختصاص في مجال التقنية والمعلوماتية أم ليس كذلك ، وسواء كان النظام المعلوماتي محصنا تقنيا بنظام الحماية أم لا.[2]

أما إذا ترتب على الدخول أو البقاء في المنظومة المعلوماتية ضرر ،كأن يتسبب الفاعل بدخوله أو بقائه في حذف لبيانات أو في تغيير لمعطيات المنظومة أو تخريب اشتغال النظام ، فقد اعتبر ذلك المشرع الجزائري في المادة 493مكررمن قبيل الظروف التي تشدد من عقوبة الجريمة، وهذا تماشيا مع جاءت به الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي صادقت عليها الجزائر.[3]

2- الاعتداء على سلامة البيانات .

وقد نصت المادة 394 مكررا1 على هذا السلوك ويتمثل في الاعتداء على النظام المعلوماتي بحد ذاته وما بداخله من معطيات ، وذلك بإدخال معطيات جديدة داخل النظام، أو إزالة معطيات، أو تدمير بيانات تقنية المعلومات، أو تعديل تلك البيانات بوجه غير مصرح به قانون أي بعير وجه حق.

3- الاعتراض غير المشروع لخط سير البيانات.

مهما كانت الوسيلة المستعملة في ذلك كقطع بث ،أو استقبال بيانات تقنية المعلومات وهذه الحالة نصت عليها المادة 7 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ولم ينص عليها المشرع الجزائري صراحة في قانون العقوبات بل نص فقط على إدخال معطيات ،أو إزالة المعطيات أو تعديلها .

---

[1]- نهلا عبد القادر المومني ، الجرائم المعلوماتية ، دار القافة للنشر والتوزيع ، الأردن ،ط2 ، سنة 2010 م، ص158.

[2]- قورة نائلة ،جرائم الحاسب الاقتصادي ،دار النهضة العربية ، القاهرة ، ط1 ، 2004م ، ص371.

[3]- المادة 6 من الاتفاقية.

4- إساءة استخدام وسائل تقنية المعلومات عمدا .

وقد نصت المادة 394 مكرر2 على هذه الصورة وتحقق في حالتين :

- **الحالة الأولى :** تتمثل في استخدام المعطيات كوسيلة لارتكاب إحدى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات التي نص عليها المشرع ، وتكون هذه المعطيات معدة خصيصا لارتكاب تلك الجرائم ، ويتمثل السلوك في تصميم برامج ،أو بحث ،أو تجميع أو توفير أو نشر ،أو الاتجار في معطيات مخزنة ،أو معالجة أو مرسلة عن طريق منظومة معلوماتية ،ومن ذلك بيع كلمة سر نظام معلومات ،أو شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلوماتي ما بقصد ارتكاب الجرائم المنصوص عليها قانونا.
- **الحالة الثانية :** وتتمثل في حيازة برامج أو بيانات متحصلة من الجرائم الماسة بالمعالجة الآلية للمعطيات ونشرها ،أو إفشائها أو استعمالها لأي غرض كان .

هذا والنتيجة في الأصل غير لازمة لتحقق جل هذه الصور ، ولا سيما في صورة الدخول إلى المنظومة المعلوماتية أو البقاء فيها ، وفي الصورة الرابعة ، بحيث تعتبر هذه الصور من الجرائم الشكلية التي تحقق بالسلوك المادي المجرد ، بحيث القيام بالفعل يعتبر بحد ذاته جريمة حتى ولو لم ينتج عن الفعل أي أثر أو ضرر ،وبالتالي فإنه لا يتصور البحث عن العلاقة السببية بين السلوك والنتيجة ،وإنما مجرد كشف واثبات السلوك ونسبته للفاعل.

كما أن الجرائم الماسة بالأنظمة المعلوماتية تعتبر من الجرائم العمدية ،التي يتطلب فيها القانون القصد الجنائي الذي يقتضي العلم والإرادة ، أي يجب أن يعلم الفاعل أنه داخل نظام معلوماتي غير مصرح له الدخول أو البقاء فيه قانونا ، أو يعلم أنه يقوم بأفعال تعتبر اعتداء على سلامة المعطيات والبيانات مع اتجاه إرادته الحرة إلى ارتكابها.

ولا يعتد القانون بالباعث الذي جعل الشخص يدخل إلى النظام المعلوماتي ،أو البقاء فيه ،حتى ولو كان بباعث نبيل كقيام الشخص بعمليات لإثبات قدرته على التحكم في التقنية المعلوماتية، أو كان من قبيل التعليم ،أو غير ذلك من البواعث النبيلة ،غير أن بعض الصور تعتبر من الصعوبة بمكان إثبات القصد الجنائي لدى مرتكبها ،ومنها صورتي الدخول و البقاء في النظام المعلوماتي بشكل عام ، باعتبار أن الشخص الذي يضبط داخل النظام باستطاعته الاحتجاج بعدم قصده الدخول أو البقاء في النظام ،وإنما هو على أهبة الخروج منه بعد اكتشافه انه داخل نظام غير

مصرح بالدخول فيه[1] ،وقد يحدث هذا في حالة إدخال شخص شيفرة أو كلمة سر بالخطأ فيجد نفسه في نظام معلوماتي غير المقصود بالشيفرة أو الدخول.

وبناء عليه فإنه إذا ارتكبت صورة من صور الاعتداء على أنظمة المعالجة الآلية للمعطيات، وتحققت عناصرها المطلوبة قانونا ، اقتضت متابعتها من قبل سلطات إنفاذ القانون وفق إجراءات خاصة تماشى وطبيعة هذه الصور من الجرائم .

المحور الثاني

التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والجهة المختصة بالنظر فيها.

لقد خص المشرع الجزائري الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بإجراءات تتناسب وطبيعة هذا النوع من الجرائم ، الذي محله الأنظمة المعلوماتية ،أو المعطيات الموجودة عليها، وغالبا ما تكون هذه الأنظمة المعلوماتية وما تتضمنه من بيانات، مختلفة عن الأشياء الأخرى التي تنصب عليها الجرائم التقليدية ، حيث الجرائم المعلوماتية تنصب على أشياء غير حسية أو بالأحرى غير مادية ، مما يقتضي معه إجراءات خاصة بالتفتيش والحفظ وكذا الحجز، كما أن مسرحها يختلف عن مسرح الجريمة التقليدية ، فهي ترتكب في فضاء افتراضي ويتم ارتكابها عن بعد فتمس عدة أمكنة في الإقليم نفسه ، أو في أقاليم أخرى فقد يكون الفاعل في مكان ، و يقع الفعل على نظام معلوماتي في مكان آخر ، وأحينا يتعدى آثار الجريمة إلى أماكن أخرى غير مكان تواجد الفاعل و مكان النظام المعلوماتي المنصب عليه ما يثير مسالة الولاية القضائية على هذه الجرائم ،وتنازع القوانين.

ونظرا أيضا لخطورة هذا النوع من الجرائم و ما تتصف به من تعقيدات ،ونظرا لارتكابها أيضا من طرف أشخاص في الغالب يكونون أكثر دراية واختصاص في مجال التقنية المعلوماتية الحديثة، و كذا قدرتهم الفائقة في اختراق الأنظمة المعلوماتية والاعتداء على محتوياتها من معطيات وبيانات ، وقدرتهم أيضا على طمس أثار الجريمة ، وأدلة إثباتها التي تدينهم ،فقد حاول المشرع الجزائري تبني مجموعة من الإجراءات الخاصة سواء من ناحية أساليب التحقيق الذي يجريه ضباط الشرطة القضائية ،أو قاضي التحقيق ،أو من ناحية الاختصاص المكاني والجهة المختصة بالنظر فيها ،وذلك قصد محاصرتها وعدم إفلات مرتكبها من المتابعة الجزائية.

أولا : التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

---

[1]- الشوا ثورة المعلومات ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية القاهرة ، ط1، 1994، ص 210.

والتحقيق قد يكون في إطار مرحلة الاستدلال أي البحث والتحري الذي يقوم به ضباط الشرطة القضائية ويسمى بالتحقيق الأولي ، وقد يكون في إطار التحقيق الابتدائي الذي يقوم به قاضي التحقيق ،ولهذا سنتطرق إلى الأساليب الخاصة بالبحث والتحري في الجرائم الماسة بالمعالجة الآلية للمعطيات ،ثم نتطرق إلى خصوصية التفتيش كإجراء من إجراءات التحقيق الابتدائي نظرا لأهميتهما في مكافحة الجريمة المعلوماتية.

أ- الأساليب الخاصة بالبحث والتحري في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

قناعة منه أن بعض الجرائم الخطيرة والمتشعبة[1] ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات لا يمكن مكافحتها أو محاربتها بطرق البحث والتحري التقليدية، فقد نص المشرع الجزائري من خلال قانون الإجراءات الجزائية والقانون المتضمن القواعد الخاصة بالوقاية من جرائم الإعلام والاتصال[2]، بأساليب خاصة من أجل البحث والتحري عن هذه الجرائم، ولعل أبرز هذه الأساليب إجراء التصنت التلفوني واعتراض المراسلات السلكية واللاسلكية والتقاط الصور، وكذا إجراء التسرب ،والمراقبة الإلكترونية.

1- التصنت التليفوني واعتراض المراسلات السلكية وللاسلكية والتقاط الصور .

وقد نصت على هذا الإجراء المادة 65 مكرر5 ق إ ج ،وإجراء التصنت التليفوني واعتراض المراسلات السلكية واللاسلكية[3] ،والتقاط الصور يسمح للسلطة المختصة متمثلة في وكيل الجمهورية ، أو قاضي التحقيق أن تأذن بتسجيل الكلام المتفوه به بصفة خاصة ، أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية ، كما يسمح باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ،وكذا يسمح بالتقاط الصور لشخص أو لعدة أشخاص يتواجدون في مكان خاص، وذلك كله بدون موافقة المعنيين الأمر الذي يطرح إشكالية مدى فعالية مثل هذا الإجراء في تحصيل الدليل لإثبات الجريمة .

---

[1]- وهي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات جرائم تبييض الأموال ، الإرهاب ،الجرائم المتعلقة بالتشريع الخاص بالصرف ، وجرائم الفساد.

[2] - القانون 09-04 المرجع السابق.

[3]- المقصود بالمراسلات السلكية واللاسلكية كل تراسل أو إرسال أو استقبال لعلامات أو إشارات أو كتابات أو صور و أصوات أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية مغنطسية. ينظر نجيمي جمال ، قانون الإجراءات الجزائية على ضوء الاجتهاد القضائي ، دار هومة ،ط3 ، 2017م ص 138.

ونظرا للحرمة التي تتمتع بها الحياة الخاصة للأفراد والتي من مظاهرها حرمة محادثاته ومراسلاته سواء كانت سلكية أو غير سلكية فقد أحاطه المؤسس الدستوري الجزائري[1] وكذا المشرع[2] بمجموعة من الضوابط ولعل أبرزها ما يلي :

- أن تقتضيه ضرورات التحري عن جريمة متلبس بها، أو إحدى الجرائم المحددة قانونا ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات..
- ضرورة حصول ضابط الشرطة القضائية على إذن مسبق من السلطة القضائية. وقد نص المؤسس الدستوري على ضرورة تعليل الأمر المستوجب المساس بسرية المراسلات والاتصالات الخاصة.
- ضرورة تنفيذ إجراء التصنت التليفوني أو اعتراض المراسلات ضابط الشرطة القضائية ،مع وجوب مراقبة عمل ضباط الشرطة القضائية.
- أن تكون مدة سريان الإذن أربعة أشهر قابلة للتجديد وحبذا لو قلص المشرع المدة التي يتعين على ضابط الشرطة القضائية القيام بهذا الإجراء بثلاثين يوما كأقصى حد قابلا للتجديد ،وذلك مثل ما فعل التشريع المصري3 ، لأن في ذلك ضمانة أكثر في عدم انتهاك حرمة الحياة الخاصة للإفراد ، كما أن ذلك يدفع ضابط الشرطة القضائية لعدم التهاون أو التقاعس في تنفيذ هذا الإجراء الحساس باعتبار انه يمس حريات الأفراد.
- ضرورة إعدام التسجيلات بعد انتهاء الغرض منها، وان كان المشرع الجزائري قد اغفل هذا الشرط بخلاف بعض التشريعات المقارنة كالتشريع الفرنسي[4]

---

[1]- المادة 46 من الدستور.

[2]- المادة 65 مكرر 5- 65مكرر7 – 65 مكرر ق إ ج

[3]- المادة 206 من قانون الإجراءات الجنائية المصري " وفى جميع الأحوال يجب أن يكون الأمر بالضبط أو الاطلاع أو المراقبة لمدة لا تزيد على ثلاثين يوما ويجوز للقاضي الجزئي أن يجدد هذا الأمر مدة أو مدداً أخرى مماثلة "

[4] -Article 100-6 Créé par Loi n°91-646 du 10 juillet 1991 - art. 2 JORF 13 juillet 1991 en vigueur le 1er octobre 1991 - Les enregistrements sont détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique.Il est dressé procès-verbal de l'opération de destruction.

https://www.legifrance.gouv.fr/affichCode

كما أن السلطات المختصة بالبحث والتحري عن الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات ملزمة بتحرير محضر عن كل عملية اعتراض أو تسجيل للمراسلات ،وكذلك عمليات وضع الترتيبات التقنية وعملية التقاط والتثبيت والتسجيل الصوتي والسمعي البصري، كما يتعين على الجهة المختصة بالبحث والتحري عن الجريمة في المحضر وصف أو نسخ المراسلات أو الصور أو المحادثات المسجلة في إظهار الحقيقة وترجمة المكالمات الأجنبية وصبها في محضر خاص ووضعها في ملف المشتبه به بارتكابه إحدى الجرائم الماسة بالمعالجة الآلية للمعطيات، وذلك كي تكون كدليل لتوجيه الاتهام ضده .

2- **المراقبة الالكترونية.**

لقد سمحت المادة03 من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بالمراقبة الإلكترونية وتجميع وتسجيل محتواها في حينها وذلك لمقتضيات حماية النظام العام ،أو لمستلزمات التحريات ،أو التحقيقات القضائية الجارية. و تشمل المراقبة الإلكترونية حسب نص المادة 02 من نفس القانون، أي تراسل أو إرسال آو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية ،ومن الحالات التي تقتضي قانونا **مراقبة الاتصالات الالكترونية** حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني ، أو مؤسسات الدولة أو الاقتصاد الوطني ، وكذالك في حالة التحريات والتحقيقات القضائية التي يتعذر معها الوصول إلى نتيجة تهم البحث الجاري دون اللجوء إلى المراقبة القضائية ما يعني أن هذا الإجراء استثناء من الأصل لما ينطوي عليه من المساس بسرية الاتصالات و حق الخصوصية الأمر الذي سبغ عليه القانون حماية خاصة ، وقيودا منها ضرورة استصدار إذن من السلطة المختصة أي وكيل الجمهورية أو قاضي التحقيق .

والسؤال الذي يتبادر للذهن في هذه المسألة هو ما مدى خضوع المراقبة الالكترونية للقيود الخاصة باعتراض المراسلات وتسجيل الأصوات والتقاط الصور المنصوص عليها في المادة 65مكرر5 من ق إ ج ، وعلى رأسها قيد المدة المتمثل في سريان الإذن المكتوب لمدة (04) أربعة أشهر قابلة للتجديد .فهل يتعين أن يتضمن الإذن بالمراقبة الإلكترونية سريانه لمدة أربعة أشهر كما هو الشأن بالنسبة للإذن الخاص باعتراض المراسلات السلكية أم يبقى على إطلاقه.؟

فبالرجوع إلى المادة 03 من القانون 09-04 المتعلقة بالوقاية من جرائم الإعلام و الاتصال فإنها تشير إلى ضرورة مراعاة القواعد المنصوص عليها في قانون الإجراءات الجزائية والقانون المتعلق

بالوقاية من الجرائم المتصلة بالإعلام والاتصال في حالة وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها ، ما يوحي أن المادة 65 مكرر5 وما تتضمنه من قيد سريان مدة اعتراض المراسلات السلكية واللاسلكية ينطبق أيضا على المراقبة الإلكترونية، وما يؤكد هذا الاستنتاج هو نص الفقرة الثالثة من المادة 4 من القانون المتعلق بالوقاية من جرائم الإعلام والاتصال التي خصصت 06 أشهر كمدة سريان الإذن بالمراقبة الإلكترونية الممنوح لضباط الشرطة القضائية إذا تعلق الأمر بالوقاية من جرائم الإرهاب أو التخريب ، أو الجرائم الماسة بأمن الدولة خلافا للحالات الأخرى المنصوص عليها في نفس المادة ، ما يقتضي خضوعها للمدة المنصوص عليها في المادة 65 مكرر5 من قانون الإجراءات الجزائية الخاصة باعتراض المراسلات السلكية واللاسلكية ،و إن كنا نحبذ لو أن المشرع نص صراحة على مدة المراقبة الإلكترونية في قانون الوقاية من جرائم الإعلام والاتصال وذلك دفعا للغموض والعموم الذي يتنافى ومبدأ الشرعية الجنائية الإجرائية. وكذلك لاختلاف طبيعة إجراء اعتراض المراسلات السلكية واللاسلكية مع إجراء المراقبة الإلكترونية .

3- التسرب .

التسرب إجراء استثنائي، يعتبر أحد الأساليب الحديثة التي سمح بها القانون لضباط الشرطة القضائية للبحث والتحري عن بعض الجرائم نظرا لتطور أساليب ارتكاب الجريمة وتشعبها ، والمقصود بالتسرب هو اختراق ضابط الشرطة القضائية ،أو احد الأعوان الوسط الذي ينشط فيه الأشخاص المشتبه في ارتكابهم لبعض الجرائم الخطيرة والتي لا يمكن الوصول إلى كشف ملابساتها ومرتكبيها إلا بهذا الأسلوب و مشاركته لهم في نشاطهم الإجرامي بقصد جمع المعلومات عن هؤلاء الأشخاص المشبوهين وعن مشروعهم الإجرامي ،وجمع الأدلة لإقامة الدعوى العمومية ضدهم على ألا يكون هذا الأسلوب محرضا على ارتكاب الجريمة ،وأن يكون ذلك كله تحت رقابة الجهات القضائية المختصة.

وقد نص المشرع الجزائري على أحكام التسرب في المادة 65مكرر11 إلى غاية المادة 65مكرر18 من قانون الإجراءات الجزائية وضمن هذه الأحكام مجموعة من الشروط والضوابط الشكلية والموضوعية باعتبار أنه إجراء في غاية الخطورة لمساسه بحق دستوري وهو حق الخصوصية ولعل أبرز هذه الشروط ما يلي:

- أن تقتضيه ضرورات التحري والتحقيق في إحدى الجرائم المنصوص عليها قانونا على سبيل الحصر[1].
- أن يكون بناء على إذن مكتوب ومسبب من وكيل الجمهورية أو قاضي التحقيق وذلك تحت طائلة البطلان.
- أن يكون سريان الإذن بالتسرب لمدة 04 أشهر قابلة للتجديد إذا اقتضت الضرورة لذلك.

وعملية التسرب يمكن تصورها في نطاق الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ،وذلك باختراق الضابط أو العون المكلف بالتسرب للمواقع والأنظمة المعلوماتية التي يشتبه أنها مسرح للأنشطة المشبوهة التي يقوم بها الجناة ، كما يمكن للضابط أو العون أن يستعمل لهذا الغرض هوية أو مواقع مستعارة ،أو الاشتراك مع الأشخاص المشبوهين في غرف الدردشة ،وكل وسيلة اتصال ،وتمكينهم من المعلومات أو المنظومات المعلوماتية المتحصلة من الجرائم المرتكبة أو المستعملة في ارتكابها ،أو قيام المتسرب بتصميم أو تجميع أو توفير ،أو نشر ،أو الاتجار في معطيات مخزنة ،أو معالجة ، أو مرسلة عن طريق منظومة معلوماتية والهدف من وراء ذلك كله الإيقاع بالأشخاص المشتبه في ارتكابهم الجرائم الماسة بالمعالجة الآلية للمعطيات ،وقيام الحجة والدليل عليهم.

وبناء على ذلك فإن الأدلة المستقاة من عملية التسرب يمكن أن تكون أساسا لإقامة الدعوى ضد المشتبه فيهم وإدانتهم ، ولكن هل يمكن أن يعول على شهادة ضابط الشرطة القضائية الذي يجري عملية التسرب تحت مسؤوليته كدليل لإدانة الأشخاص المراقبين أم لا ،ولا سيما إذا شهدوا بهويتهم المستعارة ؟

لقد أجاز المشرع الجزائري في المادة 65مكرر18 ق إ ج، سماع الضابط الذي تجري تحت مسؤوليته عملية التسرب ،وذلك كشاهد غير أنه لم يبين مدى حجية هذه الشهادة في الدعوى العمومية ، وما إن كان يجوز الاعتماد عليها كأساس لإدانة المشتبه فيهم أم لا ولذلك حبذا لو يفصح المشرع عن ذلك صراحة عن القيمة القانونية لتلك الشهادة مثلما فعلت بعض التشريعات المقارنة منها التشريع الفرنسي ، حيث نص المشرع في المادة 706-87 من قانون الإجراءات

---

[1]- جرائم المخدرات ، الجريمة المنظمة العابرة للحدود الوطنية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات جرائم تبييض الأموال ، الإرهاب ،الجرائم المتعلقة بالتشريع الخاص بالصرف ،وجرائم الفساد. المادة 65مكرر5/ المادة 56 من ق إ ج و المادة 24 مكرر1من القانون 06-01 المتعلق بالوقاية من الفساد ومكافحته، مؤرخ في 20فبراير 2006 ، المعدل والمتمم ،ج ر لسنة 2006 ، العدد 14.

الجزائية الفرنسي[1] على أنه لا يمكن النطق بالحكم على أساس التصريحات التي أدلى بها ضباط الشرطة القضائية ،أو أعوان ضباط الشرطة الذين قاموا بعملية التسرب.

ب- خصوصية التفتيش في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .

ويقصد بالتفتيش البحث عن أدلة جريمة معينة وقعت فعلا ، وذلك في مستودع السر[2] وهذا المستودع قد يكون موجودا في شخص الجاني أو في مسكنه أو في أجهزة الحاسوب أو هاتف ذكي أو أي جهاز اتصال الكتروني أو دعامة الكترونية ،وهو في الأصل إجراء من إجراءات التحقيق الابتدائي المخول لقاضي التحقيق ، غير أنه وبناء على نص المادة 44 ق إ ج يجوز استثناء لضابط الشرطة القضائية في حالة الجريمة المتلبس بها ،أو في حالة التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجريمة ، أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة والقيام بإجراء التفتيش على أن يلتزم بضوابط قانونية منها ضرورة استصدار إذن من وكيل الجمهورية أو قاضي التحقيق.

وبناء على نص المادة سابقة الذكر فإنه يجوز لضابط الشرطة القضائية في حالة إذا كان يتحرى على أفعال متلبس بها تتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات ،وهذا أمر متصور ،أو في حالة التحقيق فيها فإنه يؤذن له بتفتيش **الأشياء** ، الموجودة في المسكن[3] ، ولا شك أن أجهزة الحاسوب تدخل ضمن الأشياء الموجودة في مكان التفتيش ،كما تدخل فيها أيضا الأقراص الممغنطة وكذا الشرائح الذاكرة ،وقد قيد المشرع في المادة 45 ق إ ج عملية التفتيش بضرورة حضور صاحب الشأن وإذا تعذر عليه ذلك يكلف من طرف ضابط الشرطة القضائية بأن يعين

---

[1] - Art 706-87 Aucune condamnation ne peut être prononcée sur le seul fondement des déclarations faites par les officiers ou agents de police judiciaire ayant procédé à une opération d'infiltration.https://www.legifrance.gouv.fr/

[2] - حسام محمد سامي جابر ، نطاق الضبطية القضائية، دار الكرز للنشر والتوزيع ،مصر ،ط1 ، 2005م، ص178.

[3] - حسب نص المادة 355 ق ع ج فإنه " يعد منزلا مسكونا كل مبنى أو دار أو غرفة أو خيمة أو كشك ولو متنقل متى كان معدا للسكن و إن لم يكن مسكونا وقتذاك و كافة توابعه مثل الأحواش و حضائر الدواجن و مخازن الغلال و الإسطبلات و المباني التي توجد بداخلها مهما كان استعمالها حتى و لو كانت محاطة بسياج خاص داخل السياج أو السور العمومي".

ممثل له وإلا استدعى ضابط الشرطة القضائية لحضور التفتيش شاهدين من غير الموظفين الخاضعين إليه.

غير أنه إذا كان ضابط الشرطة القضائية بصدد البحث والتحري عن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو كانت محل التحقيق فيها ،فإنه لا تطبق تلك الأحكام[1] نظرا لخطورة الجريمة وحساسيتها ، وما تتطلبه هذه الجرائم من سرية تامة وسرعة في الضبط وذلك كي لا يعمد الجاني إلى تدمير الدليل أو إخفائه.

كما أنه لا يجوز في الأصل البدء في تفتيش المساكن ومعاينتها قبل الساعة 5 صباحا ولا بعد الثامنة مساء ،غير أنه إذا تعلق الأمر أيضا **بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات** فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل، شريطة أن يكون ذلك بناء على إذن مسبق من وكيل الجمهورية المختص.، كما يمكن لقاضي التحقيق حسب نص المادة 47 ق إ ج أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا ،وفي أي مكان على امتداد التراب الوطني أو يندب أحد ضباط الشرطة القضائية للقيام بذالك.

هذا وعملية التفتيش الخاصة بالمساكن والأماكن التي يشتبه أنها تحتوي على **أشياء** قد تقتضي **بالضرورة** تفتيش المعلومات المخزنة في الحواسيب ،أو في المنظومات المعلوماتية ،أو جزء منها ، أو وسائط تخزين ، كما يقتضي ضبط الحواسيب ، ومكوناته و كذا حجز المعطيات المخزنة ،وذلك للبحث عن الدليل الذي يتناسب مع الطبيعة التقنية للجريمة المعلوماتية التي يتم التحري عنها ،أو التحقيق فيها .

ومن الصعوبات التي قد يواجهها التفتيش في الجرائم المتعلقة بالمعلوماتية والتي قد تشكل عائقا أمام المحقق للوصول إلى الدليل الرقمي أو الالكتروني ، صعوبة اكتشافها نتيجة لإخفاء الجريمة وغياب الأثر المادي بصورة مرئية ، وصعوبة الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية ،وقدرة الجاني على تدمير دليل الإدانة بسرعة ،فضلا عن ضخامة كم المعلومات المتعين فحصها، و صعوبة الحصول عليها خاصة إذا كانت مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني ،و

---

[1]- المادة 45/ 2.

اختلاف مكان تواجد الجاني والمجني عليه [1].ولتجاوز هذه الصعوبات وغيرها فقد خص المشرع الجزائري التفتيش المتعلق بالمنظومة المعلوماتية ، وكذا المعطيات المخزنة بها بضوابط خاصة ،وذلك من خلال القانون 09-04 المتعلق بالوقاية من جرائم الإعلام والاتصال كما يلي:

1- خصوصية تفتيش المعلومات المخزنة .

لمقتضيات التحريات والتحقيقات القضائية في الأفعال التي قد تشكل اعتداء على منظومة معلوماتية والتي من شأنها تهدد النظام العام ، أو الدفاع الوطني أو مؤسسات الدولة واقتصادها، فقد أجاز المشرع الجزائري من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بجرائم الإعلام والاتصال [2] للسلطات القضائية المختصة ،وكذا لضباط الشرطة القضائية، وفي إطار قانون الإجراءات الجزائية الدخول بغرض التفتيش ولو عن بعد إلى المنظومة المعلوماتية، أو جزء منها ، وكذا المعطيات المخزنة فيها ، كما يجوز لهم الدخول إلى أي منظومة تخزين معلوماتية من شأنها تفيد في كشف الدليل ،ويجوز لهم تمديد التفتيش ليشمل منظومة معلوماتية أخرى أو جزء منها انطلاقا من المنظومة المعلوماتية الأولى ،وذلك بعلم مسبق من السلطة القضائية المختصة إذا دعت الأسباب للاعتقاد أن المعطيات المبحوث عنها مخزنة في تلك المنظومة. والأسباب المقتضية لمثل هذا التمديد تخضع للسلطة التقديرية لسلطة التحقيق أو للمحكمة.[3]

ومما يلاحظ هنا أن المشرع الجزائري لم ينص صراحة على ضرورة استصدار ضابط الشرطة القضائية إذن من السلطة القضائية لتفتيش المنظومة المعلوماتية والمعطيات المخزنة فيها، كما لم ينص على ذلك في حالة تمديد التفتيش لمنظومة معلوماتية أخرى انطلاقا من المنظومة الأولى و إنما اكتفى فقط بضرورة أن يكون ذلك بعلم السلطة المختصة ،وهناك فرق بين العلم فقط وبين الإذن الذي يجب أن يكون مكتوبا.

ولا شك أن الإذن المتطلب في تفتيش المسكن وملحقاته والمنصوص عليه في المادة 44 من قانون الإجراءات الجزائية لا يمكن إسقاطه على التفتيش الذي يتعلق بمنظومة معلوماتية ،و كذا

---

[1]- أحمد أسامة حسنية ، الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية ، مجلة جامعة الأزهر- غزة، المجلد ،91عدد خاص بمؤتمر كلية الحقوق الخامس المحكّم ص32./ نهلا عبد القادر المومني ، المرجع السابق، ص54.

[2]- المادة 5 من القانون 09-05، المرجع السابق.

[3]- مصطفى عبد الباقي ، لتحقيق في الجريمة الإلكترونية و اثباتها في فلسطين: دراسة مقارنة ،دراسات، علوم الشريعة والقانون، المجلّد ،45عدد ،4ملحق 2 ، ص291.

بما تحتويه من معلومات ،وذلك لاختلاف طبيعتهما بحيث الأول ينصب على أشياء محسوسة مادية ، بخلاف الثاني ،ولذلك حبذا لو ينص المشرع الجزائري صراحة بضرورة استصدار إذن كتابي لتفتيش أي منظومة معلوماتية أو المعطيات المخزنة فيها أو تفتيش أي دعامة الكترونية وذلك كضمانة لحماية سرية المعطيات والمعلومات المخزنة ،وكذا حماية للحق في الخصوصية المحمي دستوريا[1] ، كما يتعين أن يتضمن الإذن بالتفتيش بيان وصف الجرم موضوع البحث ،و تحديد المنظومة المعلوماتية ونوع الملفات والمعطيات المراد تفتيشها ، والأدلة المراد تحصيلها ونطاق التفتيش.

أما إذا تعلق الأمر بمعطيات مبحوث عنها مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن المشرع الجزائري لم يسمح بتمديد التفتيش إليها والنفاذ إليها مطلقا ، وجعل الحصول على تلك المعطيات مرهون بتفعيل الاتفاقيات الدولية في إطار المساعدة القضائية مع مراعاة المعاملة بالمثل. ومما تجدر الإشارة إليه بهذا الخصوص فإن الاتفاقية الأوربية المتعلقة بالجريمة الالكترونية قد أجازت للدول الأطراف النفاذ العابر للحدود إلى بيانات الكمبيوتر المخزنة في حالتين[2]:

- النفاذ إلى بيانات كمبيوتر مخزنة متاحة للعموم بغض النظر عن تواجد المعطيات جغرافيا.
- النفاذ إلى بيانات كومبيوتر مُخزنة موجودة لدى دولة طرف أخرى أو تلقيها، من خلال نظام كومبيوتر داخل أقاليمها، في حال حصول تلك الدولة الطرف على الموافقة القانونية والطوعية للشخص الذي يتوفر على السلطة القانونية للكشف عن البيانات لتلك الدولة الطرف عبر نظام الكومبيوتر المذكور.

ونظرا لما يتطلبه البحث عن الدليل الرقمي في الجرائم المعلوماتية من خبرة في مجال التقنية المعلوماتية، وكذا البرمجيات ،فقد أجاز المشرع الجزائري للسلطات القضائية المختصة تسخير كل شخص لمساعدتها في مهمة التفتيش تكون له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير الخاصة لحماية المعطيات التي تتضمنها.

كما أجاز المشرع في هذا الإطار للنيابة العامة من خلال المادة مكرر 35 من قانون الإجراءات الجزائية ، وكذا المادة 09 من المرسوم التنفيذي المحدد لشروط و كيفيات تعيين المساعدين

---

[1]- المادة 46 من الدستور الجزائري المعدل بالقانون 16-01 المؤرخ في 06 مارس 2016م ، ج ر عدد 07، بتاريخ 07 مارس 2016م.

[2]- المادة 32 من اتفاقية بودابست لسنة 2001م.

الفنيين[1] ،الاستعانة بمساعدين متخصصين للمساهمة في مختلف مراحل الإجراءات المتعلقة بالدعوى العمومية تحت مسؤولية النيابة العامة لا سيما إبداء الرأي في المسائل الفنية ، واستغلال الوثائق والمستندات ذات العلاقة بمهامه ، ومساعدة ضباط الشرطة القضائية في المسائل الفنية، ولعل الكشف عن الجرائم الماسة بالأنظمة المعلوماتية وأساليب ارتكابها يعتبر سبب كاف لاعتماد خبرة هؤلاء المساعدين الفنيين.

2- خصوصية ضبط المعلومات المخزنة.

ويقصد بالضبط في القواعد الإجرائية العامة وضع اليد على شيء مرتبط بجريمة قد وقعت فعلا ويفيد في كشف الحقيقة عنها وعن مرتكبها.[2] و قد عبر المشرع الجزائري بمصطلح الحجز على عملية ضبط المعلومات والمعطيات المبحوث عنها بعد تفتيش المنظومة المعلوماتية أو جزء منها ، باعتبار أن الضبط يرد على أشياء مادية محسوسة منقولة[3]، و من قبيل ضبط الأشياء في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ضبط المكونات المادية للحاسب الآلي كالدعامة المادية للبرامج والأسطوانات والأشرطة ، وشرائح الذاكرة وكل ما شي مفيد في التحقيق ،ويخضع ضبط الأشياء للقواعد العامة المقررة في قانون الإجراءات الجزائية ،بحيث يجب على الفور إحصاء الأشياء المضبوطة ووضعها في أحراز مختومة على ألا يجوز فتح هذه الأحراز إلا بحضور المتهم مصحوبا بمحاميه ،أو بعد استدعائهما قانونا[4] .

أما بخصوص حجز المعطيات المعلوماتية المكتشفة فإن المشرع الجزائري بين كيفية ضبط ذلك من خلال القانون المتعلق بالقواعد الخاصة للوقاية من جرائم الإعلام والاتصال[5] بحيث يتعين أن تكون هذه المعطيات المتحصل عليها مفيدة في الكشف عن الجرائم ومرتكبيها، كما يتعين نسخ المعطيات محل البحث ،وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية وتوضع هي الأخرى في أحراز مختومة ووفق ما تقتضيها المادة 84 من قانون الإجراءات الجزائية ،على أن تسهر الجهات المكلفة بالتفتيش والحجز السهر على المحافظة على سلامة ومحتوى المعطيات الموجودة

---

[1]- المرسوم التنفيذي 17-324 مؤرخ في 08 نوفمبر 2017 م ، يحدد شروط و كيفيات تعيين المساعدين المتخصصين لدى النيابة العامة وقانونهم الأساسي ، ج ر لسنة 2017 م، عدد 67.

[2]- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، ط 1،دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011،ص 168.

[3]- جلال ثروت ،نظم الإجراءات الجنائية ، دار الجامعة الجديدة للنشر ، الإسكندرية ، 1997م ،ص 457.

[4]- المادة 84 من القانون 66 – 155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

[5]- المادة 6 من القانون 09-04 المرجع السابق.

في المنظومة المعلوماتية ،ولاسيما في الأحوال التي تعمد فيه هذه السلطات إلى تشكيل أو إعادة تشكيل هذه المعطيات بوسائل تقنية بقصد استغلالها للفائدة التحقيق.

كما أجاز المشرع الجزائري في المادة 07 من القانون المتعلق بالوقاية من جرائم الإعلام والاتصال، القيام بحجز المعلومات أو المعطيات التي تتضمنها المنظومة المعلوماتية محل التفتيش والموضوعة تحت تصرف الأشخاص المرخص لهم باستعمالها وذلك من خلال منع الوصول إليها باستخدام التقنيات المناسبة إذا تعذر على السلطات المختصة القيام بالحجز عليها عن طريق نسخها في دعائم تخزين الكترونية .

ويطرح السؤال ما إذا كانت رسالة البريد الإلكتروني غير المفتوحة التي تظل في علبة البريد من مزود خدمة الإنترنت إلى أن يقوم المرسل إليه بتحميلها على حاسوبه، يجب أن تعتبر بيانات ومعلومات مخزنة أم بيانات عابرة. بحيث بموجب قانون بعض أطراف اتفاقية بودابست تعتبر رسالة البريد الإلكتروني هذه جزء من الاتصال، وبالتالي لا يمكن الحصول على مضمونها إلا من خلال تطبيق صلاحية الاعتراض، بينما تعتبر أنظمة قانونية أخرى هذه الرسالة بمثابة معطيات وبيانات مخزنة تنطبق عليها المادة 19 من اتفاقية بودبست[1] التي استوحى منها المشرع الجزائري المادتان 5 و 6 من القانون 09-04 المتضمنة إجراءات تفتيش وحجز المعطيات المخزنة.[2]

وعليه حبذا لو يبين المشرع الجزائري ما هو مناسب لهذه المسألة.

ثانيا : الجهة المختصة بالنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

نظرا لتطور الجريمة وأساليب ارتكابها بتطور تكنولوجيا الإعلام والاتصال ،فإنه كان لزاما على المشرع مواكبة هذا التطور في مكافحة الجريمة ومن اجل هذا فقد خص المشرع الجزائري الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وغيرها من الجرائم الخطيرة بمحاكم متخصصة للنظر فيها ،وذلك لما تتمتع به التركيبة البشرية لهذه المحاكم بقدر من التأهيل والتخصص في خبايا هذه الجرائم وأساليب ارتكابها و طرق الإفلات من العدالة .وتعرف هذه المحاكم بالأقطاب الجزائية المتخصصة ،كما قد تثير خصوصية الجرائم المعلوماتية مدى تأثير هذه الأخيرة على الاختصاص القضائي الجزائري ،في حالة مساس الجريمة المعلوماتية أكثر من دولة وتمسك كل دولة باختصاص قضائها بالنظر في الجريمة .

---

[1]- ينظر التقرير التفسيري لاتفاقية الجريمة الالكترونية، بودابست نوفمبر 2001م ، مجلس اوربا ،سلسلة المعاهدات الأوربية 185 ، المرجع السابق

[2]- ينظر المادة 19 من الاتفاقية بودابست لسنة 2001م المرجع السابق.

أ- اختصاص الأقطاب الجزائية بالنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

الأقطاب الجزائية المتخصصة هي تلك المحاكم المتخصصة التي يمتد الاختصاص المحلي لوكلاء الجمهورية ،وقضاة التحقيق وقضاة الحكم فيها ليشمل دوائر اختصاص محاكم أخرى ، وذلك للفصل في جرائم محددة قانونا على سبيل الحصر ،وقد حدد المرسوم التنفيذي رقم 06 -348 [1] المحاكم المتخصصة ،وذلك تطبيقا لما نصت عليه المواد 37 ف2 ، 40 /ف2 ، 329/ف5 ق إ ج ، وكذا تطبيقا للمادة 24 من القانون المتعلق بالوقاية من الفساد ومكافحته[2] التي تجيز تمديد الاختصاص في بعض الجرائم[3] لهذه المحاكم ، وتمثل هذه الأخيرة في محكمة سيدي محمد بالعاصمة، ومحكمة قسنطينة ،ومحكمة ورقلة ، ومحكمة وهران. حيث كل واحدة من هذه المحاكم يمتد اختصاصها إلى محاكم مجالس قضائية محددة قانونا[4].

وبناء عليه فإنه إذا ارتكبت **جريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات**، فإن الجهة المختصة بالنظر فيها هي المحكمة الجزائية المتخصصة بحسب المكان الذي وقعت بدائرة اختصاصه الجريمة، فإذا ارتكبت الجريمة مثلا في دائرة اختصاص المجلس القضائي لتلمسان ، أو مستغانم فإن المحكمة المختصة هي محكمة وهران ، أما إذا ارتكبت الجريمة في دائرة اختصاص المجلس القضائي لشلف أو بومرداس فإن المحكمة المختصة هي محكمة سيدي محمد لوقوع هذه المجالس في دائرة اختصاصها ودواليك.

---

[1]- المرسوم التنفيذي رقم 06-348 مؤرخ في 5 أكتوبر 2006م ، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق ،ج ر بتاريخ 8 أكتوبر 2006م ،عدد 63.

إسناد إنشاء هذه الجهات القضائية الى السلطة التنفيذية يتعارض مع ما نصت عليه المادة 141 من الدستور التي تمنح هذه الصلاحية للبرلمان فقط وبناء على قانون عضوي ، وقد اكد على هذا المجلس لدستوري من خلال **رأي رقم 01 – ر.ق.ع – م د – 05 مؤرخ في 10 جمادى الأولى عام 1426 الموافق 17 يونيو سنة 2005، يتعلق بمراقبة مطابقة القانون العضوي المتعلق بالتنظيم القضائي ، للدستور، ج ر العدد51 بتاريخ 20جويلية 2005م.**

[2]- القانون 06-01 المعدل والمتمم ، المرجع السابق.

[3]- تنص على جواز تمديد الاختصاص في الجرائم التالية جرائم المخدرات ، الجريمة المنظمة العابرة للحدود الوطنية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات جرائم تبييض الأموال ،الإرهاب ،الجرائم المتعلقة بالتشريع الخاص بالصرف ،وجرائم الفساد.

[4]- ينظر المادة 2-3-4-5 ، من المرسوم التنفيذي 06-348 ، تبين النطاق المحلي لاختصاص كل محكمة.

وقد بينت المواد 40 مكررا1 إلى 40 مكرر5 من قانون الإجراءات الجزائية كيفية اتصال المحكمة الجزائية المتخصصة بملف الدعوى ،حيث يقوم وكيل الجمهورية المختص وفق القواعد العامة بإرسال نسخة من محضر الضبطية القضائية المتعلق بالجريمة المعلوماتية إلى النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة ،وإذا رأى أن الجريمة تدخل في اختصاصه يطالب النائب العام بملف الدعوى ليحيله على وكيل الجمهورية لدى المحكمة المتخصصة ،كما يجوز له أن يطالب بملف الدعوى خلال جميع مراحل الدعوى العمومية ،بحيث إذا تم فتح التحقيق في الجريمة من طرف قاضي التحقيق العادي ،فإنه يصدر أمرا بالتخلي عن الملف لفائدة قاضي التحقيق لدى المحكمة المختصة ،ويختص رئيس المجلس القضائي الذي تقع في دائر اختصاصه المحكمة المتخصصة بالفصل بموجب أمر غير قابل للطعن في الإشكاليات التي تنشأ عن تطبيق هذه الإجراءات.

هذا كله لا ينطوي عنه أية صعوبات في تحديد الجهة القضائية المختصة ، وإنما قد تنطوي الصعوبة في حالة ما إذا كان مرتكب الجريمة خارج الإقليم الوطني ،في حين الاعتداء يكون قد وقع على أنظمة معلوماتية تقع داخل الإقليم الوطني ،ما قد ينتج عنه تنازع في الاختصاص ،وبالتالي عرقلة حسن سير عملية المتابعة الجزائية ،بل وقد يفلت الجاني من المتابعة والعقاب.

ب- أثر خصوصية الجريمة الماسة بالأنظمة المعلوماتية على الاختصاص القضائي الجزائري.

نظرا لخصوصية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات التي يعتبر الفضاء الافتراضي مسرحا لها ،وأن غالبية الأفعال المتصلة بها تمر عبر شبكات وأنظمة معلومات خارج الحدود حتى عندما يرتكبها شخص من داخل الدولة على نظام في الدولة نفسها[1]، فإن مثل هذا الوضع قد يخلق نوعا من الصعوبة في تحديد الاختصاص القضائي والقانون الواجب التطبيق، خاصة في حالة حدوث تنازع قضائي بين دول تدعي أن لها نفس الاختصاص ،ويتصور ذلك حينما يختلف مكاني الجاني والمجني عليه ،ومكان آثار الاعتداء وجنسية الجاني، كأن يكون الفاعل في دولة معينة ليس من جنسيتها ،ويقوم بالاعتداء على نظام معلوماتي يقع في دولة ثانية من جنسيته ، في حين آثار فعل الاعتداء قد يطال دولة ثالثة ورابعة من غير جنسيته.

---

[1]- عبد الله دخش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية ، دراسة مقارنة رسالة ماجستير ، جامعة الشرق الاوسط 2014م،ص86

فبناء على مبادئ الاختصاص القضائي فإن المحاكم الجزائية الجزائرية إضافة إلى اختصاصها بالنظر في الجرائم التي ترتكب داخل الإقليم الوطني، بمقتضى مبدأ الإقليمية ، فإنها أيضا تختص بالنظر في الجنايات والجنح المرتكبة في الخارج من قبل شخص يحمل الجنسية الجزائرية بمقتضى مبدأ الشخصية ، أو من طرف شخص أجنبي إضرار بأمن الدولة أو مصالحها الجوهرية ،أو أي جناية أو جنحة ترتكب إضرارا بمواطن جزائري بمقتضى مبدأ العينية.1

ما يعني ذلك أن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات قد تختص بالنظر فيها المحاكم الجزائية الجزائرية طالما مست المصالح الجوهرية للدولة وفق قواعد الاختصاص العادية . وقد أكد على ذلك القانون 09-04 المتعلق بقواعد الوقاية من جرائم الإعلام و الاتصال حيث نص على اختصاص المحاكم الجزائية الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية، أو الدفاع الوطني ،أو المصالح الإستراتيجية للاقتصاد الوطني[2].

أما في الحالة التي يتوزع فيها الاختصاص على أكثر من دولة ،وتدعي كل دولة بان لها الاختصاص فإن حل هذا الإشكال يكون بناء على ما تنص عليه الاتفاقيات الإقليمية في هذا الشأن ، ومنها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي صادقت عليها الجزائر ،حيث بمقتضى نص الفقرة الثالثة من المادة 30 من لاتفاقية فإنه إذا ادعت أكثر من دولة طرف بالاختصاص القضائي لجريمة منصوص عليها في الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو مصالحها ، ثم الدولة التي وقعت الجريمة في إقليمها ،ثم الدولة التي يكون الشخص المطلوب من رعاياها ، وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم. أما الاتفاقية الأوربية المتعلقة بالجريمة الالكترونية[3] فقد حثت الدول الأطراف عند الاقتضاء على التشاور بغرض تحديد الولاية القضائية الأنسب للمقاضاة في حالة مطالبة أكثر من دولة طرف بالولاية القضائية وهذا ما يجب أن تهتدي به الجزائر في مثل هذه الحالات.

الخاتمة

- ينظر المادة 588 ق ا ج .
- المادة 15 من القانون 09-04 المتعلق بالوقاية من جرائم الإعلام والاتصال .
[3]- المادة 22/ف5 .

من خلال هذه الورقة البحثية نستنتج ونقترح ما يلي :

1- أن الجرائم المتعلقة بالمعلوماتية تقتضي دائما مواكبتها بإجراءات خاصة أكثر مرونة وفعالية وهذا نتيجة تطور أساليب ارتكابها بتطور وسائل التكنولوجيا وتقنية المعلومات.

2- أن المشرع الجزائري حاول إعطاء نوع من الخصوصية الإجرائية للجريمة المعلوماتية تختلف عن الجرائم التقليدية عبر مراحل الدعوى العمومية أبرزها أساليب البحث والتحري المتمثلة في التصنت التلفوني واعتراض المراسلات والتسرب والمراقبة الإلكترونية إضافة إلى طرق تفتيش وضبط المعلومات المخزنة .

3- إخضاع الجرائم المعلوماتية لمحاكم متخصصة للنظر فيها ،تمتلك قدر من التأهيل والتكوين في أساليب وخبايا هذا النوع من الجرائم ،غير أن هذه المحاكم مطعون في دستوريتها بسبب عدم إنشائها من طرف البرلمان الذي له وحده صلاحية التشريع في المسائل المتعلقة بالتنظيم القضائي ما يضعف هذه الآلية القضائية.

4- حبذا لو يفصح المشرع الجزائري عن طبيعة رسالة البريد الإلكتروني غير المفتوحة التي تظل في علبة البريد من مزود خدمة الإنترنت إلى أن يقوم المرسل إليه بتحميلها على حاسوبه هل يجب أن تعتبر بيانات ومعلومات مخزنة تخضع 5 و 6 من القانون 09-04 المتضمنة إجراءات تفتيش وحجز المعطيات المخزنة أم بيانات عابرة أي جزء من الاتصال، وبالتالي لا يمكن الحصول على مضمونها إلا من خلال تطبيق صلاحية الاعتراض.

5- حبذا لو ينص المشرع الجزائري صراحة بضرورة استصدار إذن كتابي لتفتيش أي منظومة معلوماتية أو المعطيات المخزنة فيها ،أو تفتيش أي دعامة الكترونية وذلك كضمانة لحماية سرية المعطيات والمعلومات المخزنة ،وكذا حماية للحق في الخصوصية المحمي دستوريا ولا يكتفي بالقول أن يكون التفتيش بعلم مسبق من السلطة المختصة كما هو منصوص عليه في القانون 09-04 المتعلق بالوقاية من جرائم الإعلام والاتصال.

6- حبذا لو يبن المشرع الجزائري مدى حجية شهادة ضابط الشرطة القضائية الذي يجري عملية التسرب ، وان كان بإمكان القضاء بناء حكم الإدانة على شهادته فقط .

خصوصية أساليب البحث والتحري عن الجريمة المعلوماتية

The privacy of methods of research and investigation of information crime

حايطي فاطيمة طالبة دكتوراه
تحت إشراف: د.هروال نبيلة أستاذة محاضرة "أ"
كلية الحقوق والعلوم السياسية .
جامعة ابن خلدون تيارت - الجزائر

مقدمة

ساهم التطور العلمي والتكنولوجي الحديث في تطوير الجريمة بأنواعها، حيث استفاد محترفو الإجرام من الوسائل التقنية المتطورة في ارتكاب جرائمهم وبهذا قد اتخذت الجريمة أشكالا وأبعادا مختلفة وظهر ما يسمى بالجريمة المعلوماتية، أو الجريمة الإلكترونية أو جرائم الأنترنت، إذ بتعدد التسميات التي أطلقت عليها تعددت تعريفاتها، وهذا ما انجر عنه عدم وضع تعريف موحد لها، إذ نجد أن البعض عرفها على أساس وسيلة ارتكابها والبعض الآخر عرفها على أساس موضوعها أو محلها، واتجاه ثالث عرفها على أساس معيار شخصي يتمثل في الفاعل الذي ارتكبها، واتجاه رابع عرفها على أساس معيار الجمع بين المعايير السابقة حيث عرفت على أنها كل سلوك إجرامي تكون المعلوماتية وسيلة في ارتكابه أو هدفا ومحلا له، حيث تتطلب لاقترافها أن تتوافر لدى فاعلها المعرفة بتقنية الحاسب الآلي، وتميز هذه الجريمة عن نظيرتها التقليدية بعدة خصائص فنتيجة ارتباطها بتقنية المعلومات والاتصالات أصبحت من الجرائم السريعة وسهلة الانتشار لا تعترف بالحدود الجغرافية ولا الزمنية، تمتاز بطابعها الدولي العابر للحدود، ولهذا أصبح من الضروري مواجهة هذا النوع من الإجرام ومكافحته وعلى ضوء هذا لم تعد أساليب التحري التقليدية في مجال التحريات والإثبات الجنائي قادرة على التصدي لهذه الجرائم، فظهرت عدة جهود دولية وداخلية تسعى كلها لمكافحة هذا الإجرام تجلت في العديد من الاتفاقيات والمعاهدات والمؤتمرات ذات الصلة والتي أرست آليات وأساليب جديدة لمتابعة الجريمة المعلوماتية وعملت على تعزيز التعاون القضائي الدولي الذي اتخذ مظهر التعاون الأمني (الشرطي) الدولي من خلال تكاثف الأجهزة المكلفة بمتابعة هذه الجريمة في مختلف الدول، كجهاز الأنتربول

الدولي والأوروبول وغيرها، كما اتخذ هذا التعاون مظهرا آخر تجلى في المساعدة القضائية الدولية التي أقرتها عديد الاتفاقيات والمعاهدات على رأسها اتفاقية بودابست لعام 2001.

أما على المستوى الداخلي عملت جل التشريعات العربية منها والأجنبية على استحداث آليات للتصدي لهذا النوع من الإجرام من بينها المشرع الجزائري الذي عمل على تعديل بعض الأحكام والنصوص القانونية وذلك بموجب تعديل قانون الإجراءات الجزائية بالقانون رقم 22/06 بإدراج قواعد جديدة وسعت من دائرة اختصاص القضاء وضباط الشرطة القضائية باعتبارهم الجهاز المنوط به مهمة التحري عن الجرائم، واستحدث جملة من الإجراءات خاصة باعتراض المراسلات والاتصالات إلى جانب إجراء التسرب وذلك من خلال المواد من المادة 65مكرر5 إلى المادة 65 مكرر 18، كما قام باستحداث أساليب خاصة للتحري عن الجريمة المعلوماتية بموجب القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تتعلق بتفتيش المنظومة المعلوماتية وحجز المعطيات الرقمية وكذا مراقبة الاتصالات الإلكترونية، حيث جاءت هذه الإجراءات مواكبة للتطور التكنولوجي ولتتلاءم وخصوصية هذا النوع من الجرائم كونها إجراءات تعتمد بالضرورة على التقنيات الحديثة الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام أجهزة البحث والتحري عن الجرائم المعلوماتية نظرا لخصوصية التعامل معها وطبيعة الدليل فيها، وعلى ضوء ما تقدم نطرح التساؤل التالي:

ما مدى استجابة أساليب التحري الخاصة المستحدثة ضمن القوانين الإجرائية للطابع التقني للجريمة المعلوماتية؟

فرضية الدراسة: للإجابة عن التساؤل البحثي المطروح نفترض ما يلي:

تفطن المشرع للطبيعة الخاصة للجريمة المعلوماتية وما ينجر عنها من خطورة كبيرة وسارع إلى استحداث آليات لمتابعتها والقبض على مرتكبيها من خلال تعديل القوانين الإجرائية لتواكب التطور التكنولوجي الحاصل في هذا المجال والطابع التقني للجريمة في حد ذاتها.

هدف الدراسة:

نهدف من خلال هذه الدراسة إلى إبراز خصوصية التعامل مع هذا النوع من الجرائم ومدى استجابة الأساليب المستحدثة للبحث عنها لهذه الخصوصية ومعرفة مدى فعاليتها، وذلك على الصعيدين الدولي والوطني.

أهمية الدراسة:

تكمن أهمية هذه الدراسة في الحاجة إلى التصدي إلى الإجرام المعلوماتي بطرق وأساليب مستحدثة بما يتلاءم وطبيعة هذه الجريمة وما تتسم به من خصوصية تقنية كون أنها جريمة خطيرة تطال الأشخاص والأموال وأمن الدول وجب القضاء عليها والحد من خسائرها.

نطاق الدراسة:

يدور موضوع الدراسة حول خصوصية الأساليب المستحدثة في متابعة الجريمة المعلوماتية ولهذا سنعرض لأهم الجهود الدولية والداخلية (التشريع الوطني) في هذا المجال من خلال بيان الأجهزة المكلفة بمتابعة هذه الجريمة في مرحلة البحث والتحري وجمع الاستدلالات وكذا الأساليب التي استحدثها المشرع في القوانين الإجرائية في كل من القانون 22/06 والقانون 04/09.

منهجية الدراسة:

للإجابة عن الإشكال المطروح اعتمدنا المنهج الوصفي التحليلي لوصف الأجهزة المكلفة بمتابعة الجريمة المعلوماتية واختصاصاتهم في هذا المجال، و تحليل النصوص القانونية وابراز الإشكالات التي تطرحها المواجهة الإجرائية في مرحلة التحري عن هذه الجرائم. متبعين في ذلك خطة تتضمن مبحثين أساسيين:

المبحث الأول: الأجهزة المكلفة بالبحث والتحري عن الجريمة المعلوماتية.

المبحث الثاني: أساليب البحث والتحري عن الجريمة المعلوماتية في ظل القوانين الإجرائية.

الدراسات السابقة:

زاد الاهتمام بموضوع الجريمة المعلوماتية وسبل مكافحتها وخاصة في العقود الأخيرة نتيجة التطور التكنولوجي لوسائل الإعلام والاتصال الذي طرح اشكالات عديدة على المشرع وفتح المجال واسعا أمام الباحثين ومن بين الدراسات التي تناولت موضوع أساليب البحث والتحري عن الجرائم المعلوماتية والتي تتقاطع في بعض جوانبها مع موضوعها:

- دراسة "التحقيق الجنائي في الجرائم الإلكترونية" أطروحة معدة من طرف الطالب ابراهيمي جمال تضمنت اجراءات التحقيق في الجرائم الإلكترونية التقليدية منها والمستحدثة وطرق استخلاص الدليل الإلكتروني، كما تطرقت هذه الدراسة إلى الصعوبات التي تعترض جهات التحقيق وابراز الحلول المقترحة لتجاوزها.
- دراسة "آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري" مذكرة ماجستير للطالب سعيداني نعيم تطرق من خلالها إلى الجوانب القانونية للجريمة المعلوماتية،

وأساليب المواجهة التشريعية الموضوعية والإجرائية لهذه الجريمة على المستويين الدولي والداخلي.

المبحث الأول: الأجهزة المكلفة بالبحث والتحري عن الجريمة المعلوماتية.

تتفق أغلب التشريعات الدولية على إناطة مهمة البحث والتحري عن الجرائم إلى جهاز الضبطية القضائية، ولكن قد أثبت الواقع أنه لا يمكن لأي دولة لوحدها مهما بلغت من تطور في أجهزتها الأمنية متابعة الجريمة المعلوماتية والقضاء عليها لاتساما بالطابع الدولي العابر للحدود، حيث تطرح عملية البحث والتحري خارج الإقليم الوطني عدة صعوبات وتحديات أمام هذه الأجهزة، ولهذا تم إنشاء جهات أمنية دولية وداخلية تضمن الاتصال المباشر بين سلطات الأمن في جميع الدول والتبادل السريع للمعلومات بخصوص الجرائم المرتكبة والمجرمين[1] أما على المستوى الوطني خول المشرع الجزائري لهذا الجهاز اختصاصات واسعة ومتنوعة لضبط أدلة الجريمة والبحث عن مرتكبيها بغية الوصول إلى الحقيقة، غير أنه ولخصوصية الجرائم المعلوماتية تم إنشاء أجهزة خاصة ومتخصصة تعنى بمهمة التحري عن الجريمة المعلوماتية، كما منح عدة صلاحيات لهذه الأجهزة في مجال متابعة هذا النوع من الإجرام من حيث تمديد الاختصاص المحلي لها فضلا عن التنسيق الذي تقوم به مع بعض الجهات والهيئات الخبيرة في هذا المجال، وعليه ومن أجل معرفة هذه الأجهزة ومدى اختصاصها بمتابعة الجريمة المعلوماتية قسمنا هذا المبحث إلى العنصرين التاليين:

المطلب الأول: على الصعيد الدولي والإقليمي

تعتبر فكرة التعاون الأمني الدولي وسيلة ومظهرا من مظاهر التعاون القضائي الدولي الرامي لمكافحة الإجرام المعلوماتي، حيثتمثل هذا التعاون في انشاء أجهزة أمنية في مجال متابعة الجريمة المعلوماتية ومن أبرز هذه الأجهزة على هذا الصعيد نذكر ما يلي:

الفرع الأول: جهاز الأنتربول (المنظمة الدولية للشرطة الجنائية)[2] INTERPOL

---

[1] براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018، ص296.

[2] تم إحياء اللجنة الدولية للشرطة الجنائية (ICPO) من خلال عقد المؤتمر الدولي بوكسيل ببلجيكا في الفترة 1946/6/9 حيث تم على اثره نقل مقر هذه المنظمة إلى باريس وغير اسمها ليصبح المنظمة الدولية للشرطة الجنائية الأنتربول ووضع ميثاقها في الفترة من 7-1956/6/13 واعتبر نافذا من تاريخ 1956/6/13.

تعتبر أهم وأكبر منظمة شرطية في العالم أنشئت عام 1923 مكونة من قوات الشرطة ل 190 دولة مقرها بفرنسا، تهدف هذه المنظمة إلى تشجيع التعاون بين أجهزة الشرطة في الدول الأعضاء، إذ تستخدم في مجال مكافحة الجريمة المعلوماتية وسيلتين هما:

- تقوم بتجميع البيانات والمعلومات المتعلقة بالجريمة والمجرمين عن طريق المكاتب المركزية الوطنية الموجودة في أقاليم الدول الأطراف.
- تعمل على التعاون في ملاحقة مرتكبي الجرائم والقاء القبض عليهم وتسليمهم للدول التي تطالب بهم، علاوة على هذا قد أنشأت هذه المنظمة وحدات متخصصة في مكافحة الإجرام المعلوماتي تقوم بتزويد أجهزة الشرطة التابعة للدول الأعضاء بإرشادات حول التحقيق فيها وكيفيات التدريب على مكافحتها.[1]

الفرع الثاني: جهاز الأوروبول (الشرطة الأوروبية) EUROPOL

الأوروبول هو جهاز على مستوى الاتحاد الأوروبي تم انشاؤه في لكسمبورغ عام 1992 مقره مدينة لاهاي بهولندا، يعتبر حلقة وصل بين أجهزة الشرطة الوطنية للدول الأطراف في مجال التصدي للجرائم الإرهابية وجرائم المخدرات والجريمة المنظمة والإجرام المعلوماتي، يقوم هذا الجهاز بمعالجة المعلومات المرتبطة بالأنشطة الإجرامية على مستوى الاتحاد الأوروبي ودعم وسائل التحقيق لمكافحة جميع أنواع الإجرام الدولي المنظم.[2]

الفرع الثالث: جهاز الأفريبول (منظمة الشرطة الجنائية الإفريقية) AFRIPOL

تعتبر هذه المنظمة أكبر منظمة شرطة في القارة الإفريقية مكونة من قوات الشرطة ل 41 دولة، أنشئت بمبادرة من الدولة الجزائرية تم إنشاؤها في 2005/12/13 مقرها الرئيسي الجزائر العاصمة، حيث تم دعم هذه الفكرة من طرف الجمعية العامة ال 82 للمنظمة الدولية الأنتربول التي انعقدت في أكتوبر 2013 في كولومبيا، وترتكز أهم مهام وأهداف هذه المنظمة في تحديد السياسية العامة للشرطة الجنائية وتوفير التكوين وإعادة التأهيل لمختلف أجهزة الشرطة الإفريقية، وكذا ايجاد

[1] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادةالماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013/2012، ص106-107.

[2] ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2016/2015، ص 152.

الحلول في مواجهة جرائم تبييض الأموال والإرهاب والمتاجرة في المخدرات والقرصنة البحرية والجرائم المعلوماتية، فضلا عن ترقية العلاقات الثنائية بين المؤسسات الشرطية للبلدان الإفريقية.[1]

المطلب الثاني: على الصعيد الوطني

تتولى مرحلة البحث والتحري عن الجرائم بصفة عامة أجهزة الشرطة القضائية والتي حددها قانون الإجراءات الجزائية الجزائري، حيث تمارس هذه الأجهزة صلاحياتها في اجراء التحريات اللازمة بشأن الكشف عن الجريمة ومرتكبيها مقيدين في ذلك بنطاق اقليمي محدد وبنوع معين من الجرائم لا سيما الجرائم المعلوماتية ومن خلال هذه النقطة سيتم التطرق إلى مسألة الاختصاص القضائي لضباط الشرطة القضائية في مواجهة الجريمة المعلوماتية من خلال الفروع التالية :

الفرع الأول: هيكلة الضبطية القضائية

إن أعضاء الضبطية القضائية موظفون منحهم القانون صفة الضبطية القضائية، إذ قد عنى قانون الاجراءات الجزائية بتحديد أعضاء الضبط القضائي وذلك بموجب المادة 12 فقرة 1 من ق ا ج حيث تنص على :"يقوم بمهمة الضبط القضائي رجال القضاء والضباط والأعوان والموظفون المبينون في هذا الفصل[2].وعليه ينقسم رجال الضبط القضائي إلى فئتين كالآتي :

1 ضباط الشرطة القضائية :

حددت المواد 15 و15 مكرر و15 مكررا من قانون الإجراءات الجزائية الجزائري[3] ضباط الشرطة القضائية ومن خلال استقراء هذه المواد يتبين أن هناك 03 فئات ممن يتمتعون بصفة ضابط شرطة قضائية وهم :

الفئة الأولى :

هي الفئة التي تمتع بصفة ضابط الشرطة القضائية بحكم القانون وهم رؤساء المجالس الشعبية البلدية، وضباط الدرك الوطني والموظفون التابعون للأسلاك الخاصة للمراقبين ومحافظي الشرطة للأمن الوطني.

الفئة الثانية :

---

[1] ابراهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 308.

[2] أنظر المادة 12 من القانون رقم 22/06 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66_155 المتضمن قانون الإجراءات الجزائية، ج ر العدد 84، الصادرة بتاريخ 24 ديسمبر 2006.

[3] أنظر المواد 15 15 مكرر 15 مكررا من القانون 22/06 المعدل والمتمم لقانون الاجراءات الجزائية.

هي الفئة التي تمتع بصفة ضابط شرطة قضائية بناء على قرار وزاري مشترك بين وزير العدل ووزير الدفاع الوطني أو وزير الداخلية ويشترط أن يكونوا قد أمضوا 03 سنوات على الاقل في الخدمة،[1] من بينهم ذو الرتب في الدرك ورجال الدرك و غيرهم.

الفئة الثالثة:

ينتمي لهذه الفئة مستخدمو مصالح الأمن العسكري الذين يتم تعيينهم خصيصا بموجب قرار مشترك بين وزير العدل و وزير الدفاع دون اعتبار للأقدمية أو موافقة لجنة خاصة.

2 أعوان الضبط القضائي

قد حددهم قانون الإجراءات الجزائية في المادة 19 منه والتي تنص على:" يعد من أعوان الضبط القضائي موظفو مصالح الشرطة وذو الرتب في الدرك الوطني ورجال الدرك ومستخدمو مصالح الأمن العسكري الذين ليس لهم صفة ضابط الشرطة القضائية"، إلى جانب أعوان الضبط القضائي هناك بعض الموظفون المكلفون ببعض مهام الضبط القضائي أشارت إليهم المادة 14 من نفس القانون وقد أوردت المادة 21 بيانا عن هذه الفئة والتي تتكون من رؤساء الأقسام والأعوان الفنيون والتقنيون المختصون في الغابات وحماية الأراضي والولاة بموجب المادة 28 من ق ا ج، وكذا مهندسو الأشغال ومفتشو العمل وغيرهم ممن حددهم هذا القانون.[2]

وعن اختصاص ضباط الشرطة القضائية فقد مدد المشرع الجزائري من خلال القانون رقم22/06 المعدل لقانون الإجراءات الجزائية الاختصاص الإقليمي لنشاط الضبطية القضائية ليشمل كامل إقليم الوطن، إذ جاء بموجب المادة 16 فقرة 7 من ذات القانون أنه يمتد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني فيما يتعلق ببحث ومعاينة جرائم المخدرات والجريمة المنظمة عبر الحدود والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.[3]

فضلا عن هذا منح المشرع الجزائري بموجب المادة 16مكرر لضباط الشرطة القضائية ما لم يعترض وكيل الجمهورية المختص بعد إخطاره تمديد عمليات مراقبة الأشخاص الذين يوجد ضدهم

---

[1] عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، التحري والتحقيق، دار هومة للنشر، ط 2، 2011، ص 204.

[2] عفاف خذيري، الحماية الجنائية للمعطيات الرقمية، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي، تبسة، 2017_2018، ص 138.

[3] أنظر المادة 16 فقرة 7 من قانون الإجراءات الجزائية الجزائري.

مبرر مقبول أو أكثر يحمل على الاشتباه فيهم بارتكاب أحد الجرائم المنصوص عليها في المادة 16 من قانون الإجراءات الجزائية من بينها الجرائم الماسة بنظم المعالجة الآلية للمعطيات.[1]وذلك عبر كامل الإقليم الوطني.

الفرع الثاني: اختصاص الهيئات الوطنية بمتابعة الجريمة المعلوماتية

نظر للخصوصية التي تتمتع بها الجريمة المعلوماتية وفرت الدولة مجموعة من الكوادر والأجهزة المتخصصة في بحث ومعاينة الجريمة المعلوماتية وذلك إما على مستوى جهاز الشرطة أو جهاز الدرك الوطني حيث استحدث المشرع الجزائري هيئة وطنية مختصة في الوقاية من الجرائم الإلكترونية، إضافة إلى الوحدات التابعة للمديرية العامة للأمن والدرك والتي أوكلت لها عدة مهام، وعلى هذا سوف نتطرق لكل هيئة بالشرح من خلال الفروع التالية:

1 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

نص المشرع الجزائري في المادة 13 من القانون رقم 04/09 [2]على ضرورة إنشاء هيئة ذات وظيفة تنسيقية تعمل على اتخاذ الإجراءات اللازمة للوقاية من مختلف الجرائم الإلكترونية، ومساعدة السلطات القضائية في التحريات التي تجريها بهذا الشأن سنتعرف على تشكيلتها والمهام التي تضطلع بها هذه الهيئة في النقاط التالية:

أ. تشكيل الهيئة

تعرف الهيئة الوطنية للوقاية من الجرائم الإلكترونية حسب أحكام المواد 01و04 من القانون 04/09 بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي موضوعة لدى الوزير المكلف بالعدل مقرها الجزائر العاصمة وهذا طبق الأحكام المرسوم الرئاسي رقم 261-15[3] الذي يحدد تشكيلة هذه الهيئة وكيفيات سيرها وعليه تتشكل هذه الهيئة من:

- **اللجنة المديرة**

---

[1] أنظر المادة 16 مكرر من قانون الإجراءات الجزائية الجزائري

[2]القانون رقم 04/09 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 47، المؤرخة في 16 أوت 2009.

[3] المرسوم الرئاسي رقم 15_261 المؤرخ في 24 ذي الحجة 1436 الموافق ل 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 53.

تعتبر أعلى لجنة على مستوى الهيئة تتشكل من الوزير المكلف بالعدل رئيسا والوزير المكلف بالداخلية والوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال، وقائد الدرك الوطني والمدير العام للأمن الوطني، وممثل رئاسة الجمهورية وممثل عن وزارة الدفاع الوطني وقاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

- **المديرية العامة**

تنص المادة 09 من المرسوم 15-261على أنه يدير المديرية العامة للهيئة مدير عام يعين بموجب مرسوم رئاسي وتنتهي مهامه حسب الأشكال نفسها، يضطلع بعدة مهام.

- **مديرية المراقبة الوقائية الإلكترونية**

اكتف المشرع الجزائري بتعداد مهامها دون تحديد أعضائها وذلك بموجب المادة 11من المرسوم15-261.

- **مديرية التنسيق التقني**

لم يحدد القانون تشكيلتها ومن خلال تسميتها والمهام الموكلة لها يتضح أنها تتكون من مجموعة من الإداريين والتقنيين .

- **مركز العمليات التقنية والملحقات الجهوية**

نصت عليهما المواد 13و14 من المرسوم سابق الذكر بحيث تعتبر خلايا معززة بالمنشآت والتجهيزات التقنية وكذا بالمستخدمين التقنيين اللازمين لتنفيذ عمليات المراقبة التقنية للاتصالات الإلكترونية.[1]

ب.مهام الهيئة

لكل جهة من الجهات والأجهزة المشكلة لهذه اللجنة عدة مهام تندرج كلها في سياق مهمة الوقاية من الجرائم الإلكترونية وطبقا لأحكام المرسوم الرئاسي 15-261تضطلع هذه الهيئة بالمهام التالية: تعنى اللجنة المديرة بتوجيه عمل الهيئة والإشراف عليها ومراقبة وضبط برنامج عمل الهيئة وتقييمه، إضافة إلى دراسة مشاريع الميزانية والنشاطات السنوية للهيئة والمصادقة عليها، أما عن المديرية العامة فتتمثل مهمتها في السهر على حسن سيرة الهيئة وتنفيذ برامجها ونشاطاتها وضمان التسيير الاقتصادي والمالي لها، وبالنسبة لمديرية المراقبة للوقائية الإلكترونية فتعنى بتنفيذ عمليات مراقبة الاتصالات الإلكترونية من أجل كشف الجرائم المعلوماتية وتنفيذ طلبات المساعدة القضائية الأجنبية فضلا عن تزويد المصالح القضائية بالمعلومات المتعلقة بجرائم تكنولوجيا الإعلام

[1] المواد 7 9 11 12 13 14 من المرسوم سابق الذكر.

والاتصال، وتعنى مديرية التنسيق التقني بتكوين قاعدة معطيات تحليلية للإجرام المعلوماتي وإعداد الإحصائيات الوطنية المتعلقة به، والمسهلة للعمل الميداني لعناصر الضبطية القضائية.

2 الوحدات التابعة للمديرية العامة للأمن الوطني والدرك الوطني

توجد لدى المديرية العامة للأمن الوطني والدرك مجموعة من الوحدات المختصة في مجال الحفاظ على الأمن والنظام العام نذكرها فيما يأتي:

أ. الوحدات التابعة للمديرية العامة للأمن الوطني

أنشأت المديرية العامة للأمن الوطني مصلحة مركزية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على المستوى المركزي وفرق على المستوى المحلي، إضافة إلى المخبر المركزي للشرطة العلمية" بشاطوناف "بالجزائر ومخبرين جهويين بكل من قسنطينة ووهران، إذ تحتوي هذه المخابر فروع تقنية من بينها خلية الإعلام الآلي تمثل أهم مهامها في مساعدة مصالح الشرطة القضائية في التحري عن الجرائم وذلك على المستوى المحلي والدولي، فضلا عن استقبال شكاوى المواطنين وتوعيتهم وتحسيسهم بخطورة هذا النوع من الإجرام.[1]

ب. الوحدات التابعة للدرك الوطني

وضعت المديرية العامة للدرك الوطني وحدات متنوعة في مجال الحفاظ على الأمن والنظام العام ومحاربة كافة الجرائم من بين أهم هذه المصالح والوحدات المعهد الوطني للأدلة الجنائية وعلم الإجرام ب "بوشاوي" والذي يحتوي على قسم الإعلام ولإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية، بحيث يقوم بتحليل الأدلة والدعامات الالكترونية من تسجيلات صوتية وغيرها، من أجل تسهيل استغلالها في التحقيقات القضائية. [2]

المبحث الثاني : أساليب البحث والتحري عن الجريمة المعلوماتية في ظل القوانين الإجرائية.

نتيجة الإجرام المستحدث والذي أصبح يتسم بالطابع العالمي وتعدى بذلك حدود الدولة الواحدة، أصبح من الضروري وضع حد لانتشار هذا النوع من الإجرام ومكافحته بشتى السبل، وفي هذا الشأن برزت جهود المجتمع الدولي في تكثيف التعاون القضائي في مجال مكافحة هذا الإجرام، حيث تجلت هذه الجهود في عقد العديد من المؤتمرات والاتفاقيات الدولية والإقليمية

---

[1] بوكر رشيدة، الحماية الجزائية للتعاملات الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس، بلعباس، 2017، ص 329.

[2] بوكر رشيدة، الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 330.

والتي دعت صراحة إلى ضرورة وجود تعاون دولي في مجال التحري عن الجريمة المعلوماتية والتحقيق فيها، نذكر من بينها اتفاقية الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية المؤرخة في 1990/12/14 والاتفاقية الأوروبية حول الجريمة الإلكترونية لعام 2001، وكذا معاهدة بودابست لعام 2001 بشأن مكافحة جرائم نظم المعلومات والاتصالات، وغيرها من الجهود التي برزت في هذا المجال.

أما على المستوى الداخلي فقد استحدثت التشريعات آليات جديدة لمواجهة هذا النوع من الإجرام من بينها التشريع الجزائري، حيث تبنى المشرع الجزائري نصوصا قانونية جديدة وإجراءات خاصة في مجال البحث والتحري عن الجرائم المعلوماتية وذلك بموجب القانون 22/06 المعدل والمتمم لقانون الإجراءات الجزائية والقانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، منح من خلاله للسلطات القضائية أساليب مستحدثة لمتابعة هذا النوع من الجرائم، كما لم يغفل المشرع الجزائري عن النص على إجراء المساعدة القضائية الدولية ضمن أحكام القانون 04/09 مما أثار بعض التحديات أمام أجهزة التحري أمام الخصوصية التي تتمتع بها هذه الجرائم وللتفصيل أكثر قسمنا هذا المبحث إلى العناصر التالية:

المطلب الأول: إجراءات المراقبة الإلكترونية

تعتبر المراقبة (La Surveillance) من أهم مصادر التحري التي يستعان بها في بحث وتقصي الجرائم التقليدية أو المستحدثة وتعرف المراقبة الالكترونية La Cyber surveillance بأنها مراقبة شبكة الاتصالات[1] أو ذلك العمل الذي يقوم به المراقب باستخدام التقنية الالكترونية لجمع البيانات والمعلومات حول المشتبه فيه سواء كان شخصا أو مكانا أو شيئا، ويشترط في المراقب الالكتروني والذي يكون في العادة من ضباط الشرطة القضائية أن يتميز بالكفاءة التقنية العالية في مجال المعلوماتية،[2] إضافة إلى معرفة الآليات القانونية لضمان شرعية هذا الإجراء، ويتم تنفيذ المراقبة الالكترونية من خلال استهداف الاتصالات الالكترونية التي يجريها المشتبه فيه من خلال استعماله لأي وسيلة الكترونية[3] إما في شكل تراسل أو إرسال أو

[1] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الاسكندرية، مصر، 2007، ص 197_198.

[2] سمير عالية، الجرائم الالكترونية، منشورات الحلبي الحقوقية، بيروت، لبنان، ط 01، 2020، ص 463.

[3] ربيعي حسين، المراقبة الإلكترونية وحق الفرد في الخصوصية داخل الفضاء الرقمي، المجلة الأكاديمية للبحث القانوني، المجلد 13، العدد 01، 2016، ص 419.

استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أيا كانت طبيعتها تمت عن طريق وسيلة الكترونية[1].

وفي هذا السياق استحدث المشرع الجزائري جملة من الأحكام بموجب تعديل قانون الإجراءات الجزائية بالقانون رقم 22/06 والتي نصت على إجراءات مراقبة الاتصالات وتسجيلها والتقاط الصور، بموجب المواد من 65 مكرر5 إلى 65 مكرر10، واضافة إلى استحداث أسلوب التسرب المنصوص عليه في القانون 01/06 المتعلق بالوقاية من الفساد ومكافحته تحت مسمى "أسلوب الاختراق" وعليه سوف نتطرق إلى معرفة فيما تمثل هذه الإجراءات وإلى الضوابط القانونية التي تحكمها وما تحمله هذه الإجراءات من اعتداء على الحقوق والحريات الخاصة للأفراد خاصة إذا كانت هذه الحقوق مضمونة ومكفولة بالحماية الدستورية، وذلك من خلال النقاط التالية:

الفرع الأول: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

للتفصيل أكثر سنقوم بمعرفة كل إجراء من هذه الإجراءات على حدى ثم نتطرق لأهم الضوابط التي تحكمه وذلك في النقاط التالية:

01 التعريف بهذه الاجراءات:

بغرض التحري عن الجرائم الخطيرة ومن بينها الجرائم المعلوماتية أجازت المادة 65 مكرر5 من ق ا ج الجزائري لضباط الشرطة القضائية القيام بإجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور عن طريق وسائل الاتصال السلكية واللاسلكية حيث نصت المادة 65 مكرر5 على ما يلي:" إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد يجوز لوكيل الجمهورية المختص أن يأذن بما يلي : اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص، يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن، تنفذ العمليات المأذون بها على

[1] أنظر المادة 02 فقرة "و" من القانون 04/09 التي عرفت الاتصالات الإلكترونية.

هذا الأساس تحت مراقبة المباشرة لوكيل الجمهورية المختص، وفي حالة فتح تحقيق قضائي تتم العمليات المذكورة بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة".[1]

و يقصد **باعتراض المراسلات** " كل عملية مراقبة سرية للمراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه في ارتكابهم أو في مشاركتهم في ارتكاب الجريمة"،[2] حيث تكون هذه المراقبة عن طريق اعتراض أو تسجيل أو نسخ المراسلات التي هي عبارة عن بيانات قابلة للتخزين والتوزيع والاتصال والاستقبال باستعمال وسائل سلكية أو لاسلكية كالهاتف النقال والبريد الالكتروني.[3]

إضافة على هذا يدخل أيضا ضمن المراسلات محل الاعتراض "الاتصالات الالكترونية" والتي وردت في المادة 02 من قانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والتي عرفت المواصلات على أنها: " المواصلات السلكية واللاسلكية: هي كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية".

أما عن **تسجيل الأصوات** فيندرج تحت هذه العملية كل تسجيل لمحادثات شفوية يتحدث بها الأشخاص بصفة سرية أو خاصة وفي مكان عام أو خاص [4] والتي تتم عن طريق وضع ميكروفونات تلتقط الصوت وتسجله.

أما عن **التقاط الصور** فيقصد به وضع أجهزة تصوير صغيرة الحجم وإخفاؤها في أماكن خاصة لالتقاط صور تفيد في إجلاء الحقيقة وتسجيلها،[5] إضافة لذلك فان النص على وضع الترتيبات التقنية يفيد استخدام كل أنواع الأجهزة التصويرية ووسائل المراقبة المرئية المختلفة من وسائل الرؤية والمشاهدة التي تسهل عمليات الالتقاط والتثبيت وتسجيل الصور مثل الدوائر التلفزيونية المغلقة وآلات التصوير عن بعد وغيرها.

02 الضوابط التي تحكم عمليات المراقبة الإلكترونية

---

[1] أنظر المادة 65 مكرر5 من قانون الإجراءات الجزائية.

[2] عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، دار بلقيس للنشر، الجزائر، ط 04، 2019/2018، ص100.

[3] المرجع نفسه، ص 101.

[4] أحسن بوسقيعة، التحقيق القضائي، دار هومه، الجزائر، ط 8، 2009، ص 113.

[5] بن ذياب مالك، حق الخصوصية في التشريع العقابي الجزائري، مذكرة مقدمة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013/2012، ص 141.

يقصد بالضوابط القيود التي تحكم إجراءات التحري الخاصة والتي ترد على السلطة المختصة بإجرائها وتحول دون تعسفها في انتهاك حرمة الحياة الخاصة للأشخاص تمثل هذه الضوابط حسب ما جاء في ق ا ج فيما يلي:

أ. **الضوابط الموضوعية**

- **نوع الجريمة:**

المقصود هنا أن تكون هذه الإجراءات في مواجهة جرائم محددة حصرا حددها المشرع الجزائري بموجب نص المادة 65 مكرر5 من قانون الإجراءات الجزائية والتي تعتبر من الجرائم الخطيرة التي تستلزم أساليب خاصة لمواجهتها، من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات،[1] كما أضافت المادة 04 من القانون 04/09 وأكدت على الحالات التي تسمح باللجوء إلى المراقبة وهي حالة ما إذا كان الأمر يتعلق بأفعال موصوفة بجرائم الإرهاب والتخريب أو المساس بأمن الدولة.[2]

- **ضرورة اللجوء إلى هذه الإجراءات:**

وقوع جريمة من الجرائم المحددة حصرا في المادة السابقة لا يعد مبررا كافيا للجوء إلى هذه الإجراءات بل يجب فضلا عن ذلك أن تقتضي ضرورة التحري أو التحقيق ذلك إما بمناسبة جريمة متلبس بها أو بمناسبة التحقيق الابتدائي في الجرائم المحددة حصرا.

ب. الضوابط الشكلية

تمثل فيما يلي:

- **الإذن الصادر عن الجهة المختصة:**

---

[1] أنظر المادة 65 مكرر 5 من قانون الإجراءات الجزائية.

[2] تنص المادة الرابعة (4) من قانون 04/09 على الحالات التي تسمح بإجراء المراقبة فجاء فيها: " يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية:

أ. الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب. في حالة توافر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

ج. لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول الى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية .

د. في إطار تنفيذ المساعدة القضائية الدولية المتبادلة.

أوجب المشرع الجزائري وبموجب المادة 65 مكرر5 من قانون الإجراءات الجزائية الحصول على إذن قضائي من وكيل الجمهورية المختص أو قاضي التحقيق للقيام بإجراءات التحري الخاصة والوارد ذكرها في نفس المادة، إضافة إلى هذا الشرط فقد اشترط المشرع الجزائري أن يتضمن الإذن الصادر مجموعة من العناصر الأساسية وهذا ما أورده في نص المادة 65 مكرر7 من قانون ا ج بحيث أوجب أن يتضمن الإذن كافة العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة والجريمة التي تبرر اللجوء إلى هذه التدابير إضافة إلى المدة الزمنية لهذا الإذن والتي حددها بأربعة (04) أشهر قابلة للتجديد،[1] وفي حالة ما تعلق الأمر بالأفعال المنصوص عليها في الفقرة "أ" من المادة 04 من القانون 04/09 فإنه يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها إذنا لمباشرة إجراءات المراقبة الإلكترونية لمدة ستة (06) أشهر قابلة للتجديد.[2]

- **تحرير محاضر عن الإجراءات المتخذة**

أوجبت المادة 65 مكرر9 من قانون الإجراءات الجزائية على ضباط الشرطة القضائية المكلفين بالقيام بعمليات المراقبة الإلكترونية بتحرير محاضر عن كل عملية يقومون بها حيث يشمل كل محضر تاريخ وساعة بداية العملية ونهايتها، كما يرفق بملف الدعوى محضر يتضمن وصفا أو نسخة من المراسلات والصور والمحادثات المفيدة في إظهار الحقيقة وهذا ما نصت عليه المادة 65 مكرر10 فقرة01 من نفس القانون، وعند الاقتضاء إذا كانت المكالمات التي تم اعتراضها والتسجيلات الصوتية أو السمعية البصرية بلغة أجنبية تم ترجمتها بمساعدة مترجمين يتم تسخيرهم لهذا الغرض وذلك بموجب المادة 65 مكرر10 فقرة 02 من قانون الإجراءات الجزائية.[3]

الفرع الثاني: التسرب الإلكتروني:

للتفصيل أكثر سوف نتطرق بالشرح لتعريف هذا الإجراء ثم إلى الضوابط التي تحكمه:

01. التعريف بهذا الاجراء:

يعد نظام التسرب من إجراءات التحقيق الجديدة التي أرستها معظم تشريعات العالم لمواجهة الجرائم بما فيها الجريمة المعلوماتية، وقد كانت اتفاقية منظمة الأمم المتحدة المتعلقة بمكافحة الجريمة

[1] المادة 65 مكرر 7 من قانون الإجراءات الجزائية.
[2] أرجع للمادة 04 فقرة "أ" من القانون 04/09 سابق الذكر.
[3] المادة 65 مكرر 10 من قانون الإجراءات الجزائية.

المنظمة سباقة إلى احتواء هذا الإجراء بنصها على أساليب التحري الخاصة، حيث عبرت عنه بمصطلح " الأعمال المستترة" [1] وعقب تصديق الجزائر على هذه الاتفاقية تبنى المشرع الجزائري هذا الإجراء لأول مرة ضمن القانون 01/06 المتعلق بالوقاية من الفساد ومكافحته عام 2006 [2] ليبقى هذا النص جامدا لفترة معينة إلى أن تم تعديل قانون الإجراءات الجزائية بموجب القانون 22/06 أين تم تحديد معالم هذا الإجراء وتحديد ضوابطه ويقصد بالتسرب حسب نص المادة 65مكرر12 قيام ضابط أو عون الشرطة القضائية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف.

ويقصد بالتسرب الإلكتروني دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي باختراقه للمواقع الإلكترونية واشتراكه في محادثات وحلقات اتصال مباشرة مع المشتبه فيهم، والظهور بمظهر الفاعل أو الشريك أو الخافي مستخدما في ذلك أسماء مستعارة لتجنب التعرف على هويته، حيث أجاز القانون له أن يرتكب بعض الأفعال في سبيل الكشف عن الحقيقية من بينها نقل وحيازة أو تسليم أو إعطاء مواد أو وثائق متحصل عليها من ارتكاب جريمة...الخ. [3]

وحماية للضابط المتسرب حظر القانون عليه اظهار هويته الحقيقية وهو ما أكده المشرع بموجب المادة 65مكرر16، كما عاقب كل من يكشف هويته بالحبس والغرامة. [4]

02. الضوابط التي تحكمه:

نظرا لخطورة هذا الإجراء على حرمة الحياة الخاصة للأفراد فقد قيده المشرع بجملة من الضوابط الواجب مراعاتها قبل وأثناء مباشرته تمثلت فيما يلي:

أ الضوابط الشكلية:

تمثل هذه الضوابط في الإذن القضائي إذ لا يجوز للضابط المتسرب القيام بهذه العملية دون إذن مسبق من الجهات المختصة حسب أحكام المادة 65مكرر11 من ق ا ج، على أن تتم العملية تحت الرقابة المباشرة لهذه الجهات، إضافة إلى هذا وجب أن يكون الإذن الصادر مكتوبا وإلا كان الإجراء باطلا وهو ما أكدته المادة 65 مكرر15 من نفس القانون، كما يشترط أيضا أن

---

[1] ابراهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 83.

[2] القانون رقم 01/06 المؤرخ في 2006/02/20 يتعلق بالوقاية من الفساد ومكافحته، ج ر العدد 14، الصادرة بتاريخ 2006/03/08.

[3] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، المرجع السابق، ص 177.

[4] أنظر المادة 65مكرر16 من قانون الإجراءات الجزائية الجزائري.

يتضمن هذا الإذن جملة من البيانات لضمان صحته كذكر نوع الجريمة و اسم الضابط وتحديد المدة إذ لا تتجاوز أربعة (4) أشهر قابلة للتمديد حسب مقتضيات التحري.[1]

ب الضوابط الموضوعية:

تتمثل هذه الضوابط في شرطين أساسيين يتعلق الأول بتحديد نوع الجريمة والتي يجب أن تكون ضمن الجرائم التي حددتها المادة 65مكرر5 من ق ا ج من بينها الجرائم المعلوماتية، والثاني يتعلق بتسبيب الإذن الصادر بمباشرة التسرب بحيث يبين فيه الحيثيات والعناصر التي أقنعت الجهات المختصة لمنح الإذن والتي دفعت الضابط المتسرب إلى اللجوء لهذا الإجراء.[2]

المطلب الثاني:تفتيش وحجز المنظومة المعلوماتية

إلى جانب أسلوب مراقبة الاتصالات الإلكترونية الذي استحدثه المشرع الجزائري بموجب القانون 04/09 فإنه سمح بإجراء تفتيش المنظومة المعلوماتية وحجز المعطيات الرقمية المتحصل عليها وفي المقابل قيد الجهات المختصة بجملة من الضوابط التي وجب مراعاتها لعدم التعسف في هذه الإجراءات سنفصل فيها فيما يأتي:

الفرع الأول: التفتيش المعلوماتي:

يعرف التفتيش على أنه إجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة للجريمة الواقعة وإثبات وقوعها ونسبتها إلى المتهم[3] ولخطورة هذا الإجراء ومساسه بالحريات وخصوصية الأفراد وضع له المشرع ضوابط عديدة لتجنب تعسف السلطات المختصة بإجرائه وانتهاك حرمة الحياة الخاصة للأشخاص. [4] لعل أهم هذه الضوابط أو الشروط للقيام بإجراء التفتيش هو السبب القانوني له والمتمثل في وجود أدلة أو احتمال توافر قرائن في مسكن أو محل معين تدل على ارتكاب الجريمة، حيث لا يجوز إجراء التفتيش إلا بإذن مكتوب صادر عن السلطة القضائية (قاضي التحقيق أو وكيل الجمهورية) إلى أحد مأموري الضبط القضائي.[5]

---

[1] أنظر المادة 65مكرر15 من قانون الإجراءات الجزائية الجزائري.

[2] حمزة قريشي، الوسائل الحديثة للبحث والتحري في ضوء قانون 22/06 (دراسة مقارنة)، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2012/2011، ص78.

[3] عبد الفتاح بيومي حجازى، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر الإنترنت، دار الكتب القانونية، مصر، 2007، ص 192.

[4] عفاف خذيري، الحماية الجنائية للمعطيات الرقمية، المرجع السابق، ص 165.

[5] ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، دار النشر الجامعي الجديد، تلمسان، الجزائر، 2018، ص 104.

كما وقد اشترط القانون لصحة هذا الإذن توافر جملة من الشروط وفقا للمواد 44 إلى 46 منقانون الإجراءات الجزائية حيث نصت المادة 47 منه على الأوقات المسموح فيها بإجراء التفتيش، إذ لا يجوز بدء التفتيش قبل الساعة الخامسة صباحا ولا بعد الثامنة ليلا إلا بطلب من صاحب المحل أو بناء على نداءات موجهة من الداخل أو في حالات استثنائية حددتها المادة 3/47من هذا القانون والتي تعطي لضابط الشرطة صلاحية التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في أي ساعة من الليل أو النهار بإذن مسبق من وكيل الجمهورية وذلك في الجرائم الستة من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات (الجريمة المعلوماتية).

وبما أن التفتيش ما هو إلا وسيلة للإثبات المادي غايته ضبط الأدلة المادية الخاصة بالجريمة فإنه يختلف الأمر بالنسبة إلى الجرائم المعلوماتية للطبيعة الخاصة واللامادية لها، فإذا كانت الجرائم التقليدية لا تطرح أي إشكال من حيث محل التفتيش فيها فإن الجرائم المعلوماتية تطرح عدة إشكالات عن مدى جواز وقابلية المكونات الرقمية والمنطقية للحاسب الآلي لعملية التفتيش؟ وهذا ما سنحاول الإجابة عنه من خلال النقاط التالية:

01. مدى خضوع مكونات الحاسب الآلي للتفتيش

من المعروف أن الحاسب الآلي يتكون من مكونات مادية وأخرى معنوية ترتبط بغيرها من شبكات الاتصال (شبكات الأنترنت) السلكية واللاسلكية المتواجدة على المستوى المحلي والدولي، ولذلك يتطلب الأمر البحث في مدى قابلية جميع هذه المكونات للتفتيش ؟

إن تفتيش المكونات المادية للحاسب الآلي وملحقاته من لوحة مفاتيح أو طابعة أو أشياء أخرى محسوسة لا يثير أي مشاكل إجرائية أمام سلطات الاستدلال إذ يجري عليها ما يجري علي تفتيش الأشياء المادية من شروط وضمانات وبالتالي تخضع للإجراءات القانونية الخاصة بالتفتيش المنصوص عليها بموجب قانون الإجراءات الجزائية بمعنى أن حكم تفتيش المكونات المادية يتوقف على طبيعة المكان الموجودة فيه[1]، فإذا كانت موجودة في مكان خاص كمسكن المتهم مثلا كان لها حكمه ولا يجوز تفتيشها إلا في الحالات المقررة قانونا بموجب نص المادة 64 من قانون الإجراءات الجزائية وأحكام المواد من 44 إلى 47 من هذا القانون، أما إذا

[1]براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق، ص 15.

كانت موجودة في مكان عام كمحلات وغيرها فأيضا لا يجوز التفتيش إلا في الحالات التي أقرها المشرع للتفتيش في الأماكن العامة وحسب الضمانات المنصوص عليها في هذه الحالة.[1]

مدى قابلية المكونات المعنوية للحاسب الآلي للتفتيش ؟

تعرف الكيانات المنطقية للحاسب الآلي بأنها مجموعة من البرامج والقواعد المتعلقة بتشغيل وحدة معالجة البيانات[2] حيث يثار الجدل حول إمكانية وقابلية تفتيش هذه المكونات باعتبارها كيانات منطقية معنوية غير محسوسة، وفي هذا انقسم الفقه المقارن حيث ذهب الرأي الأول إلى جواز ضبط البيانات الإلكترونية المعالجة آليا ويستند في ذلك إلى أن القوانين الإجرائية جاءت عامة في نصها على التفتيش وذلك من خلال توسيع تفسير عبارة ضبط "أي شيء " لتشمل المكونات غير المادية[3] ، فيما ذهب الرأي الآخر إلى عدم جواز انطباق إجراءات التفتيش العادية على المكونات المعنوية على اعتبار أن التفتيش يهدف إلى ضبط أدلة مادية ولهذا يقترح مواجهة هذا القصور بالنص على أحكام خاصة تنظم تفتيش هذه المكونات، وهذا ما تبناه المشرع الجزائري من خلال القانون 04/09 سالف الذكر في المادة الخامسة (05) منه حيث أجاز للسلطات القضائية المختصة في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 من نفس القانون_ والتي من بينها حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الاقتصاد الوطني وللوقاية من الجرائم الماسة بأمن الدولة _ بالدخول إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المخزنة فيها وتفتيشها و ضبط الأدلة.[4]

02. مدى خضوع المنظومة المعلوماتية (شبكات المعلومات) للتفتيش

يثير تفتيش شبكات النظام المعلوماتي صعوبات كبيرة تتعلق بالطبيعة الرقمية العالمية التي تسمح بتوزيع المعلومات عبر شبكات معلوماتية في جميع أنحاء العالم، فقد يكون الموقع الفعلي لهذه المعلومات داخل اختصاص قضائي آخر في إقليم دولة واحدة أو في إقليم دولة أخرى،[5] وهو ما

---

[1] بوكر رشيدة، جرائم الاعتداءعلى نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، بيروت، لبنان، ط 1، 2012، ص 395_396.

[2] عفيفي كمال عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي القانونية، دمشق، ط 2، 2007، ص 61.

[3] بوكر رشيدة، جرائم الاعتداءعلى نظم المعالجة الآلية في التشريع الجزائري المقارن، المرجع السابق، ص 397.

[4] يزيد بوحليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل في الاقتصاد والادارة والفانون، عدد 48، ديسمبر 2016. ص84.

[5] براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق، ص 21.

يزيد الأمر تعقيدا فيثار هنا التساؤل حول مدى جواز إمداد التفتيش إلى الأنظمة المعلوماتية المتصلة بالنظام المأذون بتفتيشه والمتواجدة في دوائر اختصاص مختلفة؟ وفي هذا يمكن التفرقة بين حالتين :

أ. حالة اتصال نظام المتهم بنظام آخر موجود داخل الدولة الواحدة

بالرجوع إلى التشريع الجزائري الداخلي نجد أن المشرع قد عالج عملية تفتيش المنظومة المعلوماتية من خلال الفصل الثالث من القانون 04/09 وذلك بموجب المادة 05 فقرة 01 منه، ونظرا لخطورة الجرائم المعلوماتية فقد أجاز المشرع تمديد إجراء التفتيش داخل الإقليم الوطني ذلك بموجب المادة 05 فقرة 02 من ذات القانون.

بناء على هذا نجد أن المشرع الجزائري وزيادة على ما هو منصوص في قانون الإجراءات قد أضاف محل للتفتيش و هو المنظومة المعلوماتية أو جزء منها والمعطيات المخزنة بها، كما فصل في الإشكال المثار حول إمكانية تمديد التفتيش إلى منظومة أخرى واقعة داخل الدولة الواحدة[1] والجدير بالإشارة إلى أنه أجازت المادة 05 في فقرتها الأخيرة من ق 04/09 للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية قصد مساعدتها وتزويدها بالمعلومات الضرورية.[2]

ب. حالة اتصال نظام المتهم بنظام معلوماتي آخر موجود خارج إقليم الدولة

نتيجة الطابع العالمي للجريمة المعلوماتية قد يخزن الجناة المعلومات غير المشروعة في نظام معلوماتي خارج إقليم الدولة الواحدة وذلك لإعاقة الوصول إليه، ولهذا قام المشرع الجزائري بإجازة تمديد التفتيش إلى منظومة معلوماتية تقع خارج الإقليم الوطني إذا ما تبين لسلطات التحقيق بأن المعطيات المبحوث عنها مخزنة في تلك المنظومة، وهذا ما نص عليه في المادة 05 فقرة 04 من القانون 04/09 ،كما أضاف أنه يتم الحصول عليها بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل. [3]

وتعرف المساعدة القضائية الدولية على أنها إجراء قضائي تقوم به الدولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة معينة[4]، وتتخذ المساعدة عدة صور أهمها تبادل المعلومات

---

[1] وهذا ما يستشف من أحكام المادة 5 فقرة 1 و2 و3 من القانون 04/09 .

[2] أنظر المادة 5 في فقرتها الأخيرة من القانون 04/09.

[3] أنظر المادة 5 فقرة 3 من القانون 04/09.

[4] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، المرجع السابق، ص 89.

والإجراءات بين الدول بصدد النظر في جريمة معلوماتية، كما تسمح بالاتصال المباشر بين الأجهزة الأمنية في مختلف الدول، وتسمح أيضا بالإنابة القضائية الدولية، وقد أقرت العديد من الاتفاقيات هذا المبدأ على رأسها اتفاقية بودابست والتي أكدت على أهمية التنسيق والتعاون في مجال مكافحة الإجرام المعلوماتي بما نصت عليه من إجراءات تتعلق بتفتيش وحجز المعطيات والتحفظ عليها،[1]وبهذا الصدد نجد المشرع الجزائري ورغم نصه على مبدأ المساعدة القضائية الدولية إلا أنه أكد على إمكانية رفضها في حالة مساسها بالسيادة الوطنية أو النظام العام وهو ما جاء به في نص المادة 18 من القانون 04/09.

كما أجاز المشرع الجزائري ونظرا لخطورة هذه الجرائم وطابعها الخاص وما تتطلبه من سرعة في تعقب المجرمين لسلطات الاستدلال في حالة الاستعجال تقديم وقبول طلبات المساعدة القضائية الدولية عن طريق وسائل الاتصال السريعة مثل الفاكس أو البريد الإلكتروني، شريطة التأكد من صحتها[2].

الفرع الثاني: حجز المعطيات المعلوماتية

من المعروف أن النتيجة الطبيعية والحتمية التي ينتهي إليها التفتيش هي ضبط الأدلة التي يتم التوصل إليها في كشف الحقيقة، ونظرا لكون محل الضبط أو الحجز في مجال الجرائم المعلوماتية هو البيانات المعالجة الكترونيا، فقد ثار التساؤل حول قابلية حجز هذا النوع من البيانات؟[3]

وفي هذا انقسم الفقه إلى اتجاهين يرى الأول أن البيانات المعالجة آليا لا تصلح أن تكون محلا للحجز لانتفاء الكيان المادي عنها وبذلك لا يمكن حجزها إلا بعد نقلها من كيانها المعنوي إلى المادي الملموس، عن طرق دعامات إلكترونية،[4] حيث يستند هذا الرأي إلى أن محل النصوص القانونية المنظمة لعملية الحجز هو الأدلة المادية الملموسة، ويرى الاتجاه الثاني إمكانية حجز هذه البيانات وتسجيلها وحفظها وتخزينها على وسائط مادية وعلى إثر هذا الخلاف عمدت جل التشريعات إلى تطوير نصوصها القانونية المتعلقة بمحل التفتيش والحجز ومن بينها المشرع

[1] أدهم باسم نمر بغدادي، وسائل البحث والتحري عن الجرائم الإلكترونية، مذكرة ماجستير، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2018، ص 84.

[2]أنظر المادة 16 من القانون 04/09.

[3] بوكر رشيدة، جرائم الاعتداءعلى نظم المعالجة الآلية في التشريع الجزائري المقارن، المرجع السابق، ص 418.

[4] Kaspersen, computer crimes and others crimes against information technology in the Netherlands in ;Ulrich sieber (ed), Information Technology crime,koln etc ;carl Heymanns Verlag 1994,page 343_376.

الجزائري،[1]حيث تبنى إجراءات مستحدثة خاصة بضبط وتحريز المعطيات المعلوماتية بما يتناسب وطبيعتها اللامادية وذلك بموجب القانون 04/09، إذ اعتمد المشرع في حجز هذه المعطيات على أسلوبين مختلفين سنتطرق إليهما في شكل نقاط على النحو التالي :

.01 الحجز عن طريق نسخ المعطيات الرقمية

أجازت المادة 6 فقرة 1 من القانون 04/09 حجز المعطيات الرقمية المتحصل عليها من جراء عملية التفتيش حيث يشمل الحجز وفقا لهذه المادة الأشياء المادية والمعنوية والبيانات المعالجة الكترونيا، كما أجازت نفس المادة إمكانية حجز كل المعطياتالمخزنة التي تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، وفي حال كان ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا لقانون الإجراءات الجزائية، وأضاف المشرع في آخر المادة سالفة الذكر أنه يجب في كل الأحوال على السلطات التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، كما لها أن تستعمل كافة الوسائل التقنية لإعادة تشكيل هذه المعطيات و جعلها قابلة للاستغلال لأغراض التحقيق [2]،وذلك عن طريق عملية النسخ والنقل التي تتم بواسطة برامج متخصصة مثل برنامجLap Linkالذي يسمح بنسخ البيانات من الكمبيوتر و نقلها إلى القرص المرن.[3]

.02 الحجز عن طريق منع الوصول للمعطيات

أوجب المشرع الجزائري على السلطات المختصة بالتفتيش وحجز الأدلة استعمال التقنيات اللازمة لمنع الوصول إلى المعطيات والتي تحويها المنظومة المعلوماتية خشية منه من محو أو إتلاف أو ضياع هذه الأدلة،[4] حيث أعطت المادة 07من القانون 04/09 للجهات المختصة سلطة الأمر بالتحفظ عليها، ومن الملاحظ من هذا النص أن المشرع أجاز عملية منع الوصول للمعطيات في حالة استحالة إجراء حجزها وذلك لأسباب تقنية غير أنه لم يحدد هذه الأسباب المانعة للحجز سواء

[1]ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، المرجع السابق، ص 120.

[2]أنظر المادة 6 فقرة 3 من القانون 04/09.

[3] بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، المرجع السابق، ص 421.

[4] أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء قانون 04/09، مذكرة ماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، بجاية، 2013/2012، ص 96.

ما تعلق بالمنظومة نفسها أو ما تعلق بعملية نسخ المعطيات، كما حصر حالات اللجوء إلى الحجز عن طريق المنع في حالة واحدة فقط وهي استحالة الحجز وفق مقتضيات المادة 06 من ذات القانون، إذ يندرج تحت مفهوم منع الوصول إلى المعطيات كل إجراء تتخذه السلطات المعنية لمنع الاطلاع على المعطيات ذات المحتوى المجرم، وفي هذا السياق أجاز المشرع للسلطات المختصة بمباشرة إجراءات التفتيش والحجز أن تكلف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة وفقا لمقتضيات المادة 08 من نفس القانون.[1]

تجدر الإشارة في الأخير إلى أنه عقب أي عملية تفتيش وحجز للأدلة يتم التعامل مع المحجوزات في إطار إعادة تشكيلها وإعدادها لتقديمها إلى سلطات التحقيق والمحاكمة، وفي هذا أكد المشرع الجزائري على استعمال كل المعلومات المتحصل عليها عن طريق عمليات المراقبة الإلكترونية المذكورة سابقا في الحدود الضرورية للتحريات والتحقيقات القضائية فقط، حيث كل استعمال لها خارج هذا النطاق يقع تحت طائلة العقاب. [2]

كما نضيف إلى أن عمليات المراقبة الإلكترونية من تفتيش وحجز للمعطيات الرقمية تعترضها العديد من الصعوبات والمعوقات من بينها الحجم الهائل للبيانات المعالجة آليا، والطابع العالمي للجريمة المعلوماتية، علاوة على الخوف من الاعتداء على حقوق وحرمة حياة الأفراد الخاصة، مما يستوجب اتخاذ الضمانات اللازمة لحمايتها طبقا لما هو منصوص عليه في القوانين الإجرائية القانون 22/06 وكذا القانون 04/09 والتي أشرنا إليها سابقا.[3]

خاتمة

من خلال ما تقدم فإن موضوع البحث والتحري عن الجريمة المعلوماتية ينطوي على قدر من الأهمية القانونية والعملية، وقد تم معالجة هذا الموضوع من خلال الوقوف على معرفة الأجهزة المكلفة بمتابعة الجريمة المعلوماتية والأساليب التي استحدثها المشرع الجزائري للبحث والتحري عن ملابسات هذه الجريمة ومتابعة مرتكبيها ومدى استجابتها للخصوصية التقنية التي يتمتع بها هذا

---

[1] أنظر المادة 8 من القانون 04/09.

[2] أنظر المادة 09 من القانون 04/09.

[3] بن طالب ليندا، الدليل الإلكتروني ودوره في الإثبات الجنائي، دراسة مقارنة، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2019، ص 68.

النوع من الإجرام، متوصلين بهذا إلى جملة من النتائج المهمة وقدمنا في المقابل بعض الاقتراحات التي رأينا أنها تفيد الموضوع:

النتائج:

- اهتم المجتمع الدولي بمكافحة الجريمة المعلوماتية بشتى أنواعها وهذا من خلال الصكوك الدولية والاقليمية التي أرست بعض البنود والأحكام التي تضمنت عدة آليات وإجراءات لمتابعة هذه الجرائم ناهيك عن الأجهزة الأمنية الدولية التي ساهمت في تعزيز التعاون في هذا المجال من خلال تبادل المعلومات والإجراءات، أما داخليا فقد خول المشرع الجزائري لجهاز الضبطية القضائية اختصاصات واسعة ومتنوعة لضبط أدلة الجرائم المعلوماتية، من أهمها تمديد الاختصاص المحلي لها لرصد هذه الجرائم أينما كانت، كما عمل على انشاء أجهزة متخصصة بمهمة البحث والتحري عن الجريمة المعلوماتية باستحداث الهيئة الوطنية للوقاية من هذه الجرائم بموجب القانون 04/09 من أجل ضمان تحقيق أكبر قدر ممكن من الفعالية في مكافحة الإجرام المعلوماتي.
- إلى جانب الإجراءات التقليدية المكرسة في قانون الإجراءات الجزائية الجزائري والأساليب التي أضافها المشرع بموجب القانون 22/06 المعدل والمتمم لقانون الإجراءات الجزائية، من اعتراض المراسلات والاتصالات وأسلوب التسرب الذي تم النص عليه ضمن هذه الإجراءات، قد استحدث المشرع الجزائري آليات أخرى للتحري عن الجريمة المعلوماتية بموجب القانون 04/09 ممثلة في مراقبة الاتصالات إلكترونيا وتفتيش المنظومة المعلوماتية وحجز الأدلة الرقمية المتحصل عليها، وهي وسائل فعالة وناجعة في محاربة هذه الجريمة أثبتت فعاليتها من خلال ملائمتها لخصوصية الجريمة المعلوماتية.
- أقرت العديد من الاتفاقيات الدولية والإقليمية مبدأ المساعدة القضائية الدولية حيث أكدت على أهمية التنسيق والتعاون الدولي في مجال مكافحة الإجرام المعلوماتي، وتحقيق التوازن بين حقوق الانسان والإجراءات المتخذة لمواجهة هذه الجرائم، وحسنا فعل المشرع الجزائري من خلال تبني هذا المبدأ والنص عليه ضمن أحكام القانون 04/09 سالف الذكر.

الاقتراحات:

- نرى أن المشرع الجزائري قد واكب التطورات الحاصلة في مجال المعلوماتية بما استحدثه من أساليب جديدة للتصدي للجريمة المعلوماتية، ولكن نأمل في مشرعنا العمل على

اصدار قانون جنائي رقمي بشقيه الموضوعي الذي يتضمن مختلف أشكال الإجرام المعلوماتي وكذا الجزاءات المقررة له، وشقه الإجرائي الذي يتضمن الأساليب والآليات الفعالة في متابعة هذه الجرائم والتصدي لها بما يحقق الكشف عن الحقيقة.

- تكثيف الجهود الوطنية في مجال مكافحة الجريمة المعلوماتية والانضمام لكل الاتفاقيات والمعاهدات ذات الصلة، إضافة إلى تدريب الأجهزة الأمنية والقضائية في مجال تقنية المعلومات لتحقيق فعالية الملاحقة القضائية لهذا النوع من الاجرام المتطور والخطير جدا.

سلطة القاضي الجزائي اتجاه الدليل الرقمي.

.The power of the criminal judge toward digital evidence

د لرقط عزيزة

كلية الحقوق

جامعة العربي بن مهيدي أم البواقي- الجزائر.

مقدمة

إن التقدم التكنولوجي الحاصل في مجال التقنية الحديثة جعل من العالم قرية صغيرة تتدفق بين أرجائها المعلومات في سهولة و سرية و غزارة، و يتبادل الناس فيها أخبارهم و يحصلون فيها على أية معلومات يريدونها بسرعة فائقة، حتى وصف هذا العصر بعصر المعلوماتية، إلا أنه خلف آثارا سلبية نتيجة الاستعمال غير المشروع لهذه التقنية، إذ طالت هذه الاعتداءات قيما جوهرية تخص الأفراد والمؤسسات والدول في كافة نواحي الحياة الاقتصادية والأمنية والثقافية، و خلفت بدورها شعورا في النفوس بعدم الأمان وغياب الثقة بسبب التهديد بالاعتداء على الأفراد وأمنهم.

ونظرا لتنوع أساليب ارتكاب هذه الجرائم، وتزايد مخاطرها وحجم الخسائر الناجمة عنها إذ أصبحت تشكل مصدرا لتهديد الاقتصاد والأمن الوطني من جهة بالنسبة للدول التي ترتكز مصالحها الحيوية على التقنية بشكل عام وعلى المعلوماتية بشكل خاص، لاسيما بعد انتقالها في إطار عصر المعلومات إلى اقتصاد المعلومات الذي يرتكز على المعرفة والاتصالات وليس فقط على القوى العاملة والموارد البشرية، ومن جهة أخرى المؤسسات التي تعتمد اعتمادا كليا على الحاسبات الآلية لتسيير أعمالها وتنظيم حساباتهـــــا، و أيضا الأفراد الذين طالت ذمتهم المالية وحياتهم الخاصة وملكيتهم الفكريـــــــة، إذ أصبحت هذه الجرائم ظاهرة عامة.

و هذا ما دفع بالمشرع الجزائري على غرار التشريعات المقارنة التدخل و سد الفراغ التشريعي في هذا المجال بجرم ما عده" المساس بأنظمة المعالجة الآلية للمعطيات" بموجب تعديل قانون العقوبات من خلال استحداث القسم السابع مكرر من المادة 394 مكرر إلى غاية المادة 394 مكرر7،إلا أن هذا التعديل لم يتطرق إلى جميع صور الاعتداءات في مجال المعلوماتية خاصة تلك التي تلحـــــــــق بالأفــــــــــــــراد و أموالهم، و بالتالي فإن المشرع أوكل مهمة إسباغ عدم المشروعية لهذه الاعتداءات وفقا لنصوص قانون العقوبات للقضاة، و ذلك بإعمال سلطتهم التقديرية سواء في تقدير مدى تطابق الأفعال المرتكبة في مجال المعلوماتية مع النص

القانوني، أو تقدير الأدلة التي تنسب من خلالها الواقعة إلى مرتكبها، و هذا ما يعد خرقا صارخا لمبدأ المشروعية و ما يترتب عنه من نتائج خاصة ما تعلق بحظر القياس و التفسير الضيق لنصوص قانون العقوبات.

وأمام هذه المخاطر و التغيرات تحورت إشكالية موضوع سلطة القاضي الجزائي اتجاه الدليل الرقمي في ما مدى صلاحية و شرعية الدليل الرقمي المتحصل عليه بواسطة الانترنت و قبوله و اعتماده في تكوين قناعة القاضي الجزائي ؟.

و عليه فإن موضوع الدراسة الحالية نهدف من خلاله تحقيق جملة من الأهداف قد تساعد في فهم ما تم استحداثه في مجال المعلوماتية و الإحاطة ببعض جوانبه السلبية، ومن بين تلك الأهداف نذكر مايلي:

- التعرف على الدليل الرقمي من خلال تحديد المقصود منه و تبيان خصائصه.
- تبيان المشكلات الإجرائية في الحصول على الدليل التقني.
- بيان الضوابط و القيود الواردة على حرية وسلطة القاضي الجزائي في قبول وتقدير القوة الثبوتية للدليل الرقمي في الجريمة المعلوماتية.

و جملة الأهداف السابق الإشارة إليها جاءت من الأهمية التي يكتسيها موضوع سلطة القاضي الجزائي اتجاه الدليل الرقمي باعتباره من الموضوعات التي لا غنى عنها في القانون الذي يرمي إلى إيجاد الصيغ الملائمة للاستفادة من التقدم العلمي دون المساس بالحقوق و الحريات الأساسية، إلا أن خاصية البعد الدولي التي تمتع بها الجريمة المعلوماتية أثار العديد من المشاكل القانونية و الصعوبات العملية التي وقفت عائقا أمام أجهزة العدالة في مواجهتهم لهذا النوع المستحدث من الجرائم لا سيما الأجهزة القضائية و مسألة إثبات الجرائم المرتكبة عن طريق الأنترنت و مدى مصداقية الأدلة المتحصل عليها بواسطة الانترنت و قبولها و اعتمادها في تكوين قناعة القاضي الجزائي كما هو الحال بالنسبة للدليل الرقمي الذي يتم الحصول عليه وفق خطوات معقدة كون مستودعه وسائل الكترونية.

و من ثم فإن الإجابة على الإشكالية السابق إثارتها اقتضت الضرورة الجمع بين المنهجين التحليلي و الوصفي، منهج تحليلي من خلال تحليل النصوص القائمة وتبيان مدى ملائمتها و كفاءتها اتجاه الدليل الرقمي، أما المنهج الوصفي فيتبين من خلال وصف طبيعة الدليل الرقمي و تحديد خصائصه و مميزاته.

و للإحاطة بشتى جوانب هذه الدراسة قسمنا الموضوع إلى مطلبين خصصنا المطلب الأول للدليل الرقمي محل القبولأين تناولنا في الفرع الأول مفهوم الدليل الرقمي، أما الفرع الثاني فتطرقنا إلى أساس قبول الدليل الرقمي في الإثبات، في حين خصصنا الفرع الثالث إلى القيود الواردة على حرية القاضي في قبو الدليل الرقمي، أما المطلب الثاني فتناولنا فيه سلطة القاضي الجزائي في الاقتناع بالدليل الرقمي حيث تم تقسيمه إلى فرعين تطرقنا في الفرع الأول إلى حرية القاضي الجزائي في تقدير الدليل الرقمي، و في الفرع الثاني تعرضنا للضوابط التي تحكم اقتناع القاضي الجزائي بالدليل الرقمي، ثم خاتمة تعرضنا فيها إلى أهم النتائج و الاقتراحات التي تم التوصل إليها.

المطلب الأول/

الدليـــــــل الرقــــــــي محل القبول:

يعد قبول الدليل الجزائي بصفة عامة والدليل الرقمي بصفة خاصة الخطوة الإجرائية الأولى التي يمارسها القاضي اتجاهه، وذلك قبل البدء في تقديره للتأكد من مدى صلاحيته وملاءمته لتحقيق الغرض الذي وجد لأجله، وقبول الدليل على هذا النحو يتسع ويضيق تبعا للمبادئ التي تقوم عليها أنظمة الإثبات السائدة التي قد تمنح للقاضي الحرية أو تقيدها.

والقاضي الجزائي في هذه المرحلة يهدف إلى التيقن من مدى مراعاة الدليل لقاعدة المشروعية، والتي بدونها لا يمكن له أن يرتب الآثار القانونية، وإنما يترتب عن إهمالها بطلان الدليل وما ترتب عنه من إجراءات، إلا أن حداثة الأدلة الرقمية كوسائل إثبات في المادة الجزائية تتطلب أولا تحديد مفهوم الدليل التقني، وعليه نتناول في هذا المطلب مفهوم الدليل الرقمي في فرع أول، ثم نعرض في الفرع الثاني إلى أساس قبول القاضي الجزائي للدليل الرقمي، وفي الفرع الثالث نتطرق للقيود الواردة على حرية القاضي في قبول الدليل الرقمي.

الفرع الأول/مفهوم الدليـــــــل الرقـــــي:

يعد الدليل بالمفهوم العام من المسائل ذات الأهمية الكبيرة في الوصول بالقاضي إلى النطق بالإدانة أو البراءة، وإذا كان الدليل وفق مفهومه المادي لا يثير أي إشكال في إثبات الجريمة بصفة عامة، إلا أن الأمر يختلف بالنسبة للجريمة المعلوماتية التي تنصب على محل ذو طبيعة معنوية، مما يترتب على إثباتها إقامة الدليل الذي يتلاءم وطبيعتها وهو الدليل الرقمي وهو ما يلزم وضع تعريف لهذا الأخير مع تبيان خصائصه.

أولا/ تعريف الدليل الرقـــــــــــــــي:

حاولت التعريفات التي وضعت للدليل الرقمي استيعاب النوع المستحدث من الأدلة بالرغم من حداثته وارتباطه بالتقنية الرقمية الحديثة، إذ عرف على أنه:" معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحاسوبية المخزنة في أجهزة النظم المعلوماتية وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيـــق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جاني أو مجني عليه"[1].

كما عرف أيضا بأنه:" الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات ونبضات مغناطيسيــــــــــة أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال أو الرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ و تطبيق القانون"[2].

أما المنظمة العالمية لدليل الكمبيوتر (IOCE) في أكتوبر 2001 فعرفته بأنه" المعلومات ذات القيمة المحتملة أو المخزنة أو المنقولة في صورة رقمية"[3].

والملاحظ على هذه التعريفات أن البعض منها قد ألحق الدليل الرقمي بمفهوم برامج الحاسب الآلي على الرغم من اختلاف كل واحد عن الآخر، حيث تم اعتبار هذا الدليل كبيانات يتم إدخالها للحاسب الآلي وهو ما يتوافق مع تعريف برامج الحاسب الآلي[4]، كما أن وظيفة برامج الحاسب الآلي تمثل في تشغيل الحاسوب وتوجيهه إلى حل المشاكل ووضع الخطط المناسبة، كما يوجد من البرامج الخاصة من تساهم في استخلاص الدليل مثل برامج معالجة الملفات[5]، أما الدليل الجزائي

---

[1]- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات حلبي الحقوقية، بيروت، 2012، ص 383.

[2]- ممدوح عبد الحميد عبد المطلب ، البحث و التحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، المحلة الكبرى، 2006، ص88.

[3]- مصطفى محمد موسى ، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة، 2009، ص 213.

[4]- رشيدة بوكر، المرجع السابق، ص384.

[5]- أشرف عبد القادر قنديل ، الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة، الاسكندرية، 2015، ص125.

الرقمي فله أهمية كبرى كأساس في كيفية حدوث مختلف الجرائم المعلوماتية بهدف إثباتها ونسبتها إلى مرتكبها[1].

كما حصرت بعض التعريفات السابقة الدليل الرقمي في ذلك الذي يتم استخراجه من الحاسب الآلي، وهو ما يعد تضييقا لدائرة الأدلة التقنية التي أثبت العلم ظهور وسائل تقنية أخرى كالهاتف النقال، والبطاقات الذكية والمساعد الرقمي الشخصي وغيرها من الأجهزة التي يمكن استخلاص الدليل الرقمي منها[2].

وتأسيسا على الملاحظات السابقة يمكن استخلاص تعريف للدليل التقني على أنه:" معلومات مخزنة في النظام المعلوماتي وملحقاته، أو متنقلة عبره، تكون في شكل نبضات مغناطسية أو كهربائية ممكن تجميعها و تحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة لتظهر في شكل مخرجات ورقيـــــــــــــــــــــــــة أو إلكترونية أو معروضة على شاشة النظام المعلوماتي أو غيرها من الأشكال لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها"[3].

ثانيا/ خصائص الدليل الرقمي:

إن البيئة الرقمية التي يعيش فيها الدليل التقني بيئة متطورة بطبيعتها، فهي تشمل على أنواع متعددة من البيانات الرقمية التي قد تكون منفردة أو مجتمعة وتصلح لأن تكون دليلا للإدانة أو البراءة[4]، ومنه فإن هذه البيئة انعكست على هذا الدليل و أضفت عليه خصائص يمكن تفصيلها فيما يلي:

أ/ الدليل الرقمي دليل علمي:

يتكون الدليل الرقمي من بيانات ومعلومات ذات طبيعة الكترونية غير ملموسة لا تدرك بالحواس العادية، حيث لا يمكن الحصول و الاطلاع عليه سوى باستخدام الأساليب العلمية، لذلك يتعين على رجال الضبطية القضائية والخبراء أثناء التعامل مع الدليل الرقمي سعيا وراء كشف الحقيقة و إثبات الجريمة المعلوماتية أن تبنى عملية البحث على أسس علمية دقيقة، فالدليل العلمي يخضع لقاعدة ضرورة تجاوبه مع الحقيقة كاملة وفقا لقاعدة أن القانون مسعاه العدالة أما العلم فمسعاه

---

[1]- عائشة بن قارة مصطفى ، حجية الدليل الالكتروني في مجال الاثبات الجنائي، دار الجامعة الجديدة، الاسكندرية، 2010، ص61.

[2]- أشرف عبد القادر قنديل، المرجع السابق، ص125.

[3]- رشيدة بوكر، المرجع السابق، ص385.

[4]- عائشة بن قارة مصطفى، المرجع السابق، ص61.

الحقيقة[1]، و عليه فإن الدليل الرقمي ذوطبيعة علمية فلا يجب أن يخرج هذا النوع من الأدلة عما توصل إليه العلم الرقمي و إلا فقد معناه[2].

ب/ الدليل الرقمي من طبيعة تقنية و رقمية:

الدليل الرقمي هو دليل تقني لوجوده بالبيئة التقنية فلا يمكن تواجده خارجها، وعليه يتم التعامل معه من قبل تقنيين مختصين في البيئة الافتراضية والأنظمة المعلوماتية، كما أن الدليل الرقمي ليس كالدليل العادي باعتباره نبضات رقمية تجلى قيمتها في إمكانية تعامل التقنيين مع دعائمها المادية[3]. والطبيعة التقنية للدليل الرقمي ميزته عن الدليل المادي من حيث قابليته للنسخ، إذ تعتبر الأدلة الرقمية المنسوخة المطابقة للأصل لها ذات القيمة العلمية، وهذه الخاصية لا تتوافر في أنواع الأدلة الأخرى مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل من الضياع والتلف والتغيير، وتحديد ما إذا كان الدليل الرقمي قد تم التلاعب أو العبث فيه أو تعديله، وذلك لإمكانية مقارنته بالأصل عن طريق استخدام البرامج والتطبيقات الصحيحة[4]، خاصة و أن الدليل التقني سهل التعديل و الاتلاف أو إدراج معلومات رقمية أخرى في مستندات بسرعة فائقة[5].

ج/ الدليل الرقمي دليل متنوع ومتطور:

يتخذ الدليل الرقمي أشكالا مختلفة، إذ أن مصطلح الدليل الرقمي يشمل كافة البيانات الرقمية الممكن تداولها رقميا، وتكون بينها وبين الجريمة رابطة من نوع ما، وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني، كما أن تنوع الأدلة الرقمية يتحقق في الحالة التي تكون فيها البيانات غير مقروءة من خلال ضبط مصدر الدليل مثل ماهو الحال في المراقبة عبر الشبكات والخوادم،

---

[1]- عمر محمد بن يونس، الدليل الرقمي، ندوة الدليل الرقمي، جامعة الدول العربية، المنظمة العربية للتنمية الإدارية، القاهرة 5-8 مارس 2006، ص7، منشور على الموقع: http://unpan1.un.org/intradoc/groups/public/documents/arado/unpan026347.pdf تاريخ الاطلاع: 2020/03/15.

[2]- فتحي محمد أنور عزت، الأدلة الالكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، الطبعة الأولى، دار الفكر والقانون، القاهرة، 2010، ص648.

[3]- رشيدة بوكر، المرجع السابق، ص390.

[4]- فتحي محمد أنور عزت، المرجع السابق، ص649.

[5]- رشيدة بوكر، المرجع السابق، ص388.

أو في الحالة التي يكون فيها الدليل مفهوما يمكن للشخص قراءته كما لو كان وثيقة رقمية معدة بنظام word أو مقطع من فيديو أو صورة أو ملف رقمي من ملفات نظام التشغيل[1].

د/ الدليل الرقمي يصعب التخلص منه:

وتعد من أهم خصائص الدليل الرقمي، بل هي ميزة يتميز بها الدليل التقني عن غيره من الأدلة العلمية الأخرى، فالقاعدة في هذا الإطار والتي تسري على كل ما يتعلق بهيكلة تكنولوجيا المعلومات، أن الاتصال بشبكات المعلوماتية أو إجراء أية عمليات معالجة بالأجهزة الرقمية يصعب التخلص منها ولو كان ذلك عن طريق الاستعانة ببرامج المسح والحذف الخاصة[2]، إذ توجد من برامج حاسوبية لها وظيفة استعادة البيانات و المعلومات التي تم حذفها[3].

وترتيبا على ذلك فإن العديد من التشريعات الداخلية نصت على ضرورة الاحتفاظ بمعلومات الزبائن الذين قدموا على الاتصال بشبكة الأنترنت لمدة معينة، وهو ما أكده المشرع الجزائري من خلال المادة 11 من القانون رقم 04/09[4] التي تنص على أنه " تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل.........".

ولقد كانت قضية إيران كونترا« IRAN – CONTRA » سنة 1986 من أول القضايا التي أبرزت هذه الخاصية للدليل الرقمي وما يتمتع به من صلابة، إذ أدرك المسؤولون الأمريكيون في هذه القضية عدم وجود تطابق في مقارنة الدليل الرقمي بالدليل الورقي، ذلك أن هذا الأخير يمكن التخلص منه بتمزيق الورقة التي تحمله في حين أن الدليل الرقمي يمكن إعادته للحياة حتى وإن كان قد تعرض للإزالة، وفي هذه القضية أثناء التحقيق مع الكولونيل "أوليفرنورد" تمت استعادة

---

[1]- عائشةبن قارة مصطفى، المرجع السابق، ص63.

[2]- فتحي محمد أنور عزت، المرجع السابق، ص654.

[3]- خلف حمد ميسون الحمداني، مشروعية الأدلة الإلكترونية في الإثبات الجنائي، مجلة كلية الحقوق، جامعة النهرين، المجلد 18، العدد 2، كانون الثاني 2016، ص201. منشور على الموقع: https://www.iasj.net/iasj?func=article&aId=109238،تاريخ الإطلاع:2020/03/15.

[4]- القانون رقم 04/09 المؤرخ في 14 شعبان عام 1430ه الموافق ل 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها الجريدة الرسمية العدد 47 المؤرخة في 25 شعبان عام 1430 ه الموافق ل 16 غشت 2009.

جميع الرسائل الالكترونية المتعلقة بالجريمة بعد أن قام هذا الكولونيل بحذفها من حاسوبه، إذ لم يكن يعلم هذا الأخير أن هذه الرسائل يمكن استعادتها عن طريق النسخ المحفوظ في النظام[1].

الفرع الثاني/

أساس قبول الدليل الرقمي في الإثبات:

إن طبيعة نظام الإثبات السائدة في الدولة هو المعيار الذي يتحدد على أساسه موقف القوانين المقارنة فيما يتعلق بسلطة القاضي في قبول الدليل التقني، وفي هذا الإطار نجد أن أنظمة الإثبات لا تخرج عن ثلاث فئاتو هي نظام الأدلة القانونية، القوانين الأنجلوساكسونية حيث تقيد من حرية الإثبات في مرحلة الفصل بالإدانـــة أو البراءة، أما في مرحلة تقدير العقوبة فيسود مبدأ حرية الإثبات، أما الفئة الثالثة فهي القوانين ذات الصياغة اللاتينية التي تبنت مبدأ حرية الإثبات، وعليه فالقاضي الجزائي له سلطة في قبول جميع الأدلة ما لم يستبعدها المشرع بنص خاص كالقانون الفرنسي من خلال المادة 427 من قانون الإجراءات الجزائية، والقانون الجزائري في المادة 212 من قانون الإجراءات الجزائية، وما دام المشرع الجزائري استند لمبدأ حرية الإثبات في المواد الجزائية[2]، لذا سوف نقتصر الدراسة على النظام اللاتيني كأساس لقبول الدليل التقني، إذ نتناول فيه المقصود بمبدأ حرية الإثبات، والنتائج المترتبة عنه:

أولا/المقصود بمبدأ حرية الإثبات:

تعد حرية الإثبات في المادة الجزائية من المبادئ الأساسية المستقرة في نظرية الإثبات، ويقصد بمبدأ حرية الإثبات إعطاء حرية للأطراف في تقديم أي دليل يرونه مناسبا لأجل إثبات صحة ما يدعونه و ذلك لأسباب و مبررات تماشي و الدعوى الجزائية التي تنصب أصلا على وقائع مادية أو معنوية نفسية يستحيل ويصعب الحصول على دليل مسبق لها[3]، ،وقد أقر المشرع الجزائري مبدأ حرية الإثبات في المادة الجزائية من خلال المادة 212 من قانون الإجراءات الجزائية التي تنص على أنه:" يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال

1- نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستر، جامعة الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، 2012-2013، ص125.

2- الأمر155/66 المؤرخ في 18صفر عام 1386ه الموافق ل8 يونيو 1966 يتضمن قانون الإجراءات الجزائرية المعدل و المتمم، الجريدة الرسمية العدد49، المؤرخة في 21 صفر عام 1386 الموافق ل11 يونيو1966.

3- أشرف عبد القادر قنديل، المرجع السابق، ص196-197.

التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص و لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه".

ثانيا/ النتائج المترتبة على تطبيق مبدأ حرية الإثبات:

إن إعمال مبدأ حرية الإثبات يجعل للقاضي الجزائي حرية في توفير وقبول وتقدير الدليل بما في ذلك الدليل التقني، وعليه سنوضح في هذا النطاق دور القاضي الجزائي في توفير وقبول الدليل التقني.

أ/ الدور الإيجابي للقاضي الجزائي في توفير الدليل التقني:

بالرغم من أن عبء الإثبات يقع على عاتق النيابة العامة، وبالتالي هي المنوطة بتقديم دليل الإدانة، و على المتهم نفي هذا الدليل بكل المكنات المخولة له، إلا أن ذلك ليس مفاده عدم تدخل القاضي البتة في هذا الإطار[1]، فالقاضي الجزائي يؤدي دورا هاما بل له أكثر الأدوار أهمية في الدعوى الجزائية وبصفة خاصة في شأن عملية الإثبات، ولتوضيح ذلك يتعين أولا تحديد مفهوم هذا الدور ثم مظاهره.

1- مفهوم الدور الإيجابي للقاضي الجزائي في توفير الدليل الرقمي:

يقصد به عدم التزام القاضي بما يقدمه الخصوم من أدلة و إنما له من السلطة اتخاذ جميع الإجراءات التي تفيد في الكشف عن الحقيقة الواقعية.

وعليه فإن دور القاضي الجزائي يختلف عن دور القاضي المدني الذي يقتصر دوره على قبول الأدلة المقدمة من الخصوم في الدعوى وفقا لما نص عليه القانون، ولا يمكنه اتخاذ أي إجراء من تلقاء نفسه للبحث عن الأدلة أو توجيه الأطراف إلى تقديم دليل معين.

وترتيبا على ما تقدم و نظرا لهيمنة النظام التنقيبي على الإجراءات الجزائية في القانون الجزائري، فإن دور القاضي إيجابي في مرحلة التحقيق والفصل في الدعوى الجزائية، لأن المقصود بالقاضي ليس قضاء الحكم فحسب، وإنما يشمل أيضا قضاء التحقيق لأن مشكلة الإثبات تثور في أي مرحلة تمر بها الدعوى العمومية[2].

[1]- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2007، ص37.

[2]- أشرف عبد القادر قنديل، المرجع السابق، ص198.

2- مظاهر الدور الإيجابي للقاضي الجزائي في توفير الدليل الرقمي:

يتضح الدور الايجابي الذي يلعبه القاضي الجزائي في توفير الدليل الجزائي الذي يساعد في كشف الجريمة ونسبتها إلى مرتكبها، من خلال تمكين القاضي من اتخاذ الإجراءات التي يراها ضرورية ومناسبة للفصل في موضوع الدعوى المعروضة أمامه، ويتحقق الدور الايجابي للقاضي الجزائي في مواد الجنايات التي خول فيها المشرع الجزائري لرئيس المحكمة اتخاذ كافة الإجراءات التي تفيد في الكشف عن الحقيقة، إذ لا يرد عليه أي قيد سوى ضميره وهو ما أقرته صراحة المادة 286 من قانون الإجراءات الجزائية الجزائري المقابلة للمادة 310 فقرة 1 من قانون الإجراءات الجزائية الفرنسي[1]، أما في مواد الجنح والمخالفات فيتجسد الدور الايجابي له من خلال سلطته في سماع و إحظار الشهود، حسب أحكام المادة 220 إلى المادة 233 من قانون الإجراءات الجزائية الجزائري، أو الاستعانة بالخبراء إذا ما اعترضته مسألة من المسائل الفنية وهو ما أقره المشرع الجزائري في المواد 143 و219 من قانون الإجراءات الجزائية. وتطبيقا على الجريمة المعلوماتية، فإن القاضي الجزائي و لأجل الوصول إلى الحقيقة له توجيه الأمر لمزود الخدمة لأجل تقديم كافة المعطيات التي تسمح بالتعرف على المجرم المعلوماتي، وكذا عناوين المواقع المطلع عليها وهو ما أشارت إليه المادة 11 من القانون 04/09.

كما يتحقق أيضا الدور الايجابي للقاضي الجزائي في البحث عن الدليل الرقمي من خلال سلطته وصلاحيته في إصدار الأمر باعتراض الاتصالات السلكية واللاسلكية متى تبين جديته وملاءمته لسير الدعوى، وهو ما أقره المشرع الجزائري من خلال المادتين 3 و 4 من القانون 04/09.

وتعد الخبرة الفنية والتقنية من أقوى مظاهر التعامل القانوني والقضائي مع ظاهرة تكنولوجيات المعلومات، فهي تؤدي دورا لا يستهان به خاصة مع نقص المعرفة القضائية الشخصية في مجال الأنظمة المعلوماتية، إذ يعتبر مثلا البحث عن المعلومات داخل النظام المعلوماتي من الأمور البالغة التعقيد التي تتطلب وجود خبير لا سيما في حالة التشفير وغيرها من الوسائل الفنية[2]، وهو

---

[1] - Article 310 alinéa 1 du code procédure pénal dispose que « Le président est investi d'un pouvoir discrétionnaire en vertu duquel il peut, en son honneur et en sa conscience, prendre toutes mesures qu'il croit utiles pour découvrir la vérité. Il peut, s'il l'estime opportun, saisir la cour qui statue dans les conditions prévues à l'article 316 ».

[2]- Myriam quéméner, Cyber menaces, entreprises et internautes, Ed Economica,2008, p :229.

ما تناولته المادة 14 فقرة ب من القانون 04/09 التي تنص على أنه: "مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام و الاتصال بما في ذلك تجميع المعلومات و إنجاز الخبرات القضائية".

ب/ الدور الإيجابي للقاضي الجزائي في قبول الدليل الرقمي:

إن مرحلة قبول الدليل الرقمي تلي مرحلة البحث عن الدليل وتقديمه من قبل جميع الأطراف (القاضي، النيابة العامة، المتهم)، وعليه فإن القاضي لا يقوم بتقدير إلا الدليل المقبول الذي تم الحصول عليه وفقا لمبدأ الشرعية الإجرائية، أو بعبارة أخرى فإن القاضي لا يقوم بتقدير الدليل إلا إذا كان مشروعا وتم الحصول عليه بطرق مشروعة[1].

والجدير بالذكر في هذا المجال إثارة مسألة أساسية تتمثل في مدى تأثير الطبيعة الرقمية للدليل التقني على قبوله من طرف القاضي الجزائي، خاصة وأن المألوف هو قبول الدليل المادي لأنه يعبر عن وضعية مادية ملموسة كالورق المكتوب أو البصمة الوراثية[2] أو الحدوث العيني للواقعة، أما الدليل التقني فهو ذو طابع رقمي يعبر عن تعداد غير محدود لأرقام ثنائية موحدة، فطبيعة الدليل التقني لا تعبر عن قيمة أصلية بمجرد رفع محتواه على الأنترنت حيث يتواجد في كل مكان يتم استدعاءه منه[3].

وترتيبا على ذلك فإن المشكلة تقوم بصورة واضحة في الحالة التي يقوم فيها المتهم بمحو و إزالة الدليل التقني عن بعد، وما يتم الحصول عليه عن طريق المراقبة الالكترونية ما هو إلا نسخة فقط عن الدليل، و عليه هل يمكن اعتبار هذا الأخير دليل أصلي وبالتالي يقبل طرحه أمام القضاء؟، وذات الإشكال في الحالة التي يسترد فيها الدليل بعد محوه وذلك عن طريق خاصية الإلغاء.

و من ثم يتعين على المشرع الجزائري النص صراحة على افتراض الأصالة في الدليل التقني خاصة في الحالة التي يتم استرجاعه بعد محوه و إزالته، وإن كان يستفاد من بعض النصوص اعترافه بما ينتج مثلا عن الحاسب الآلي ونذكر من ذلك ما نصت عليه المادة 323 مكررا1 من

---

[1]- أشرف عبد القادر قنديل، المرجع السابق، ص200.

[2]- تعرف البصمة الوراثية حسب المادة الثانية الفقرة الأولى من القانون 03/16 على أنها" التسلسل في المنطقة غير المشفرة من الحمض النووي".

[3]- رشيدة بوكر، المرجع السابق، ص487.

القانون10/05[1] أين أقر المشرع أن الإثبات بالكتابة في الشكل الالكتروني مثل الإثبات على الورق.

الفرع الثالث/

القيود الواردة على حرية القاضي في قبول الدليل الرقمي:

إذا كان مبدأ حرية الإثبات يمنح للقاضي الحرية في بناء قناعته على أي دليل يراه مناسبا بما فيه الدليل التقني، إلا أن هذه الحرية ليست مطلقة في جميع الحالات بل هناك قيود وحدود قد تفرض على القاضي حتى لا تعم الفوضى ويسود تسلط القضاة في التشدد أو التساهل مع الجـــــــــــــاني، أو ينحرف عن الغرض الذي يبتغيه المشرع وهو الوصول إلى الحقيقة الفعلية في الدعوى التي تمثل الهدف الأسمى لقانون الإجراءات الجزائية.

وترتيبا على ذلك فإن العديد من التشريعات تدخلت في تحديد الأدلة التي يستوجب على القاضي اعتمادها في إثبات بعض الجرائم وهو ما يتفق مع مبدأ نظام الإثبات المقيد، وهو ما أخذ به المشرع الجزائري في بعض الجرائم كما هو الحال في جريمة الزنا المنصوص عليها بموجب المادة 341 من قانون العقوبات[2] إذ حددت أدلة الإثبات مسبقا.

إلا أن هناك قيد عام يحد من حرية القاضي في قبول الدليل وهو مشروعية الدليل بما فيها الدليل التقني، لأن مبدأ شرعية الجرائم والعقوبات التي يقوم عليه بنيان القانون الجنائي انعكس على قواعد الإثبات الجزائي التي يفترض خضوعها هي الأخرى لمبدأ الشرعية، لذا سنعرض أولا إلى تعريف مشروعية الحصول على الأدلة التقنية، وثانيا نتناول قيمة الدليل غير المشروع.

أولا/ تعريف مشروعية الحصول على الأدلة التقنية:

تعرف المشروعية على أنها:" الالتزام والتقيد بأحكام القانون في شكله ومضمونه العام، فهي تهدف إلى تقرير ضمانة أساسية وجدية لحماية الحريات والحقوق الشخصية للأفراد ضد تعسف السلطة ومن التجاوز عليها في غير الحالات التي يسمح فيها القانون بذلك، من أجل حماية النظام الاجتماعي وبنفس القدر تحقيق حماية مماثلة للفرد ذاته"[3].

---

[1]- القانون رقم 10/05 المؤرخ في 13 جمادى الأولى 1426 ه الموافق ل 20 يونيو 2005 يعـــــــــــدل ويتمم الأمر 58/75 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني، الجريدة الرسمية العدد 44، المؤرخة في 19 جمادى الأولى عام 1426ه الموافق ل 26 يونيو 2005.

[2]- الأمر156/66 المؤرخ في 18 صفر عام 1386ه الموافق 8 يونيو1966 يتضمن قانون العقوبات المعدل و المتمم، الجريدة الرسمية العدد49، المؤرخة في المؤرخة في 21 صفر عام 1386 الموافق ل 11 يونيو 1966.

[3]- هلالي عبد اللاه أحمد، المرجع السابق، ص104.

ولقد وضعت الدساتير الوطنية نصوصا تتضمن ضوابط لشرعية الإجراءات التي تضمن وتكفل الحريات الأساسية وحقوق الإنسان و أكد ذلك التعديل الدستوري الجزائري المؤرخ في 06 مارس 2016 [1] باستحداثه الفقرة الثانية من المادة 46 التي تنص على أنه:" لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميها القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة .

لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية ويعاقب القانون على انتهاك هذا الحكم حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي ويعاقب على انتهاكه ".

ويتضح من خلال هذا النص أن المشرع يؤكد دوما على الحماية التي يكفلها مبدأ شرعية العقوبات والجرائم، كما أن هذه القاعدة يمتد أثرها من حيث التطبيق إلى تنظيم الإجراءات التي تتخذ ضد المتهم على نحو يضمن احترام الحقوق والحريات الفردية، وتعرف هذه القاعدة بالشرعية الإجرائيـــــــــــــــــــــــة أو قاعدة مشروعية الدليل الجزائي، ويقصد بها مطابقة الإجراءات المتخذة لما نص عليه القانون، ولا يقتصر ذلك عند هذا الحد بل يتعدى إلى مراعاة حقوق الإنسان والمواثيق والاتفاقيات الدولية وقواعد النظام العام والآداب العامة السائدة في المجتمع، بالإضافة إلى المبادئ التي استقرت عليها المحكمة العليا، وبصفة عامة مراعاة الأنظمة الثابتة في وجدان المجتمع المتحضر[2].

وقياسا على ذلك فإن جمع الأدلة المتحصلة عليها من الوسائل الالكترونية التي تخالف القواعد والمبادئ التي تنظم كيفية الحصول عليها تعد باطلة، ومن ثم بطلان الدليل المستمد منها تطبيقا لقاعدة ما بني على باطل فهو باطل، وهو ما يؤثر على نتيجة الدعوى خاصة في الحالة التي يكون فيها الدليل الباطل هو الدليل الوحيد في ملف الدعوى مما يتعين القضاء بالبراءة، وعليه لا يجوز للقاضي أن يقبل في إثبات إدانة المتهم دليلا تقنيا تم الحصول عليه بناء على تفتيش نظام معلوماتي باطل.

ومن جهة أخرى يكتسب هذا القيد أهمية كبرى نتيجة التقدم الهائل الذي تحقق في السنوات الأخيرة في شأن الوسائل الفنية للبحث والتحقيق، والتي تسمح أكثر فأكثر باختراق مجال الحياة

---

[1]- القانون رقم 16-01 المؤرخ في 26 جمادى الأولى عام 1437 الموافق ل 6 مارس 2016 المتضمن تعديل الدستور، الجريدة الرسمية العدد14، المؤرخة في 27 جمادى الأولى عام 1437 الموافق ل 07 مارس 2016.

[2]- رشيدة بوكر، المرجع السابق، ص490.

الخاصة للأفراد[1]، كالمراقبة الالكترونية التي استحدثها المشرع الجزائري بموجب القانون 04/09 وما لها من مساس أكثر فأكثر بحقوق الأفراد وحرياتهم إذا لم يحسن استخدامها، وهو ما يترتب عليه الإضرار بالعدالة.

ثانيا/ قيمة الدليل التقني غير المشروع:

الأصل أن الدليل الجزائي المعتد به هو الدليل الذي يتم الحصول عليه وفق طرق مشروعة، ومن ثم فإن الأدلة التي يتم الحصول عليها وفق إجراءات مشوبة بالبطلان هي أدلة غير مشروعة، وعليه يثور التساؤل في هذا المطاف هل تختلف قيمة الدليل الرقمي غير المشروع في الإثبات بحسب الغاية منه في الدعوى العمومية؟ لأن الدليل قد يكون دليل إدانة أو دليل براءة وبالتالي سوف نعرض لهاذين الحالتين:

1- بالنسبة لدليل الإدانة:

تطبيقا لمبدأ قرينة البراءة فإنه يستوجب معاملة المتهم على أنه بريئ في مختلف مراحل الدعوى العمومية إلى غاية صدور حكم بات في حقه، ويشترط في الأدلة التي تؤسس عليها الإدانة أن تكون مشروعة، ومن ثم فإن الأدلة التي تم الحصول عليها بطرق غير مشروعة أو بوسيلة مخالفة للقانون تعتبر أدلة باطلة بما فيها الدليل الرقمي، ومن أمثلة الطرق غير المشروعة التي يمكن أن تستعمل في الحصول على الدليل التقني إكراه المتهم المعلوماتي على فك الشفرة للدخول إلى النظام المعلوماتي أو إجباره للحصول على كلمة السر اللازمة لأجل الولوج إلى المعلومات الموجودة داخل النظام المعلوماتي، أو المراقبة الالكترونية عن بعد بدون إذن قانوني صادر من القاضي المختص تدخل أيضا في إطار عدم المشروعية عملا بأحكام المادة 41 من قانون الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2].

وبالتالي حتى يصل القاضي إلى حكم الإدانة يجب أن يعتمد أدلة مستمدة من إجراءات صحيحة ومشروعة، فإذا ما شاب هذه الإجراءات سبب من أسباب البطلان ترتب عنه بطلان الحكم الذي يعتمدها.

---

[1]- أشرف عبد القادر قنديل، المرجع السابق، ص207.

[2]- المرسوم الرئاسي رقم 261/15 المؤرخ في 24 ذي الحجة 1436 الموافق ل 08 أكتوبر2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد53 المؤرخة في 24 ذي الحجة عام 1436 الموافق ل 08 أكتوبر 2015.

2- **بالنسبة لدليل البراءة:**

إذا كان دليل الإدانة المتحصل عليه بالطريق غير المشروع دليل باطل لا يمكن اعتماده للفصل في الوقائع المعروضة على القاضي، إلا أن دليل البراءة نلتمس اختلاف حول مدى اشتراط المشروعية، و هو ما جعل الفقه يختلف في إمكانية الأخذ به من عدمه، وعليه سوف نعرض لكل اتجاه نبين ما هي الأسس والتبرير الذي قدمه في ذلك.

الاتجاه الأول:

يذهب هذا الاتجاه إلى أن المشروعية في الحصول على الدليل لازمة سواء كان دليل إدانـــــــــــــــــــة أو دليل براءة، وهو ما يستخلص من نصوص قانون الإجراءات الجزائية التي تناولت بطلان الإجراءات التي يستمد منها الدليل بطريق غير مشروع بصفة عامة دون أي تفرقة بين ما إذا كان دليل إدانـــــــــــــــــــة أو دليل براءة، ومن ثم لا يصح أن يفلت دليل البراءة من قيد المشروعية الذي هو شرط أساسي في أي تشريع لكل اقتناع سليم[1].

الاتجاه الثاني:

وعلى نقيض الاتجاه الأول يرى هذا الاتجاه أن شرط المشروعية لازم في دليل الإدانة دون دليل البراءة، ويؤسس ذلك على أن المحكمة لا تحتاج إلى اليقين في إثبات البراءة بل يكفي قيام الشك باعتباره من نتائج قرينة البراءة، وهو ما يمكن الوصول إليه من خلال أي دليل ولو كان غير مشروع، كما أن بطلان الدليل المستمد بوسيلة غير مشروعة شرع أساسا لحماية حرية المتهم، ومن ثم فإنه من غير المعقول أن ينقلب عليه، كما أن التمسك بعدم قبول دليل البراءة اعتمادا على عدم مشروعيته يؤدي إلى وقوع القاضي في خطأ مفاده إدانة بريء وإفلات مجرم من العقاب[2].

الاتجاه الثالث:

ويرى مؤيدي هذا الاتجاه ضرورة التفرقة بين ما إذا كان دليل البراءة قد تم الحصول عليه نتيجة جريمة معاقب عليها قانونا، أو كان الحصول عليه نتيجة سلوك يشكل مخالفة لقاعدة إجرائية، فإذا كانت الطريقة الأولى هي التي تم بها الحصول على الدليل وجب إهداره وعدم الاعتداد به، أما

[1]- عائشة بن قارة مصطفى، المرجع السابق، ص220.

[2]- أشرف عبد القادر قنديل، المرجع السابق، ص210.

إذا كان الحصول على الدليل قد تم عن طريق مخالفة قاعدة إجرائية فيصح الاستناد إليه لأجل تبرئة المتهم[1] لتحقيق الغاية من تشريع البطلان.

وفي إطار الترجيح بين الاتجاهات الثلاثة نرى أن الاتجاه الأخير هو الأكثر تحقيقا للعدالة، لأنه اتجاه متوازن ويتوافق مع الأصل العام ومبدأ قرينة البراءة، ذلك أنه من غير المقبول القول باستبعاد دليل البراءة الذي يؤكد براءة المتهم لمجرد أنه لم يستوف بعض الإجراءات الشكلية اللازمة، وفي المقابل لا يمكن اعتماد دليل البراءة الذي كان نتيجة لجريمة تم ارتكابها، لأن القول بخلاف ذلك مفاده اعتماد دليل البراءة حتى وإن كان الحصول عليه نتيجة ارتكاب جريمة، و هو ما يفتح المجال أمام الأشخاص والمتهمين في زيادة معدلات الجرائم لأجل الحصول على دليل البراءة.

المطلب الثاني/

سلطة القاضي الجزائي في تقدير الدليل الرقمي:

أخذ المشرع الجزائري بما هو سائد فقها فيما يتعلق بسلطة القاضي الجزائي في تقدير الدليل، التي يحكمها مبدأ حرية القاضي الجزائي في تكوين عقيدته وقناعته، مما يترتب عليه نتيجتان تتمثل النتيجة الأولى في حرية القاضي في قبول الأدلة والنتيجة الثانية تجلى في حرية القاضي في تقدير الأدلة.

وذهب الفقه في هذا المطاف للقول بالنتيجة الثانية دون النتيجة الأولى، لأن هذه الأخيرة هي مسألة قانونية لتدخل المشرع في تحديد النموذج القانوني للدليل الذي يخضع للسلطة التقديرية للقاضي.

وإذ كان مبدأ الاقتناع القضائي يخول حرية واسعة في تقدير الأدلة إلا أن هذه الحرية قد ترد عليها بعض القيود والضوابط، وعليه يقتضي تناول سلطة القاضي في تقدير الدليل التطرق لحريته في الاقتناع بالدليل الرقمي في الفرع الأول، ثم التعرض للضوابط التي تحكم اقتناع القاضي بالدليل الرقمي في الفرع الثاني.

الفرع الأول/

حرية القاضي الجزائي في الاقتناع بالدليل الرقمي:

---

[1]- رشيدة بوكر، المرجع السابق، ص494.

مما لاشك فيه أن الدليل الرقمي ما هو إلا صورة من صور الدليل العلمي له حجيته في الإثبات بما يتمتع به من موضوعية و حياد و كفاءة تقوم على قواعد علمية حسابية قاطعة لا تقبل التأويل مما يقوي يقينيته، ويساعد القاضي في الوصول إلى الحقيقة الواقعية، وبالتالي التقليل من الأخطاء القضائية[1].

وعليه فإن ظهور الدليل الرقمي قد زاد من دور الإثبات العلمي الذي يتم اللجوء فيه لأصحاب الخبرة الذين أصبح لهم دور فعال في هذا المجال، خاصة أمام غياب الثقافة المعلوماتية، والذي أدى في المقابل إلى تضاؤل دور القاضي الجزائي في تقدير الدليل الرقمي الذي يتميز بالموضوعية والحياد والكفاءة، مما يجعل للخبير القول الفاصل الذي يتعين على القاضي الخضوع له.

وترتيبا على ذلك نتناول في هذه المسألة الطبيعة العلمية للدليل الرقمي وأثرها على اقتناع القاضي أولا ثم نتطرق إلى مدى تأثير مشكلات الدليل الرقمي على اقتناع القاضي ثانيا.

أولا/ الطبيعة العلمية للدليل الرقمي وأثرها على اقتناع القاضي:

قبل الحديث عن الطبيعة العلمية للدليل الرقمي وأثرها على اقتناع القاضي الجزائي، يتعين أولا تحديد وبيان مضمون مبدأ الاقتناع القضائي ومفهومه في الإثبات، ثم توضيح قيمة الدليل الرقمي في الإثبات.

أ/مفهوم مبدأ الاقتناع القضائي:

من المقرر قانونا أن لمحكمة الموضوع كامل الحرية في أن تستمد اقتناعها وتكوين عقيدتها على أي دليل تطمئن إليه طالما أن له مأخذ صحيح من أوراق الدعوى، كأن يؤسس القاضي أو يعتمد على أقوال شهود الإثبات ويستبعد أقوال شهود النفي إذا لم يثق بما شهدوا به، لأن له كامل الحرية في تقدير القوة التدليلية في الإثبات، و عليه سنتناول المقصود مبدأ الاقتناع القضائي ثم نطاق هذا المبدأ.

1- تعريف مبدأ الاقتناع القضائي:

لم يحدد المشرع كيفية تكوين القاضي لاقتناعه وعقيدته لأنها ترتبط بالنشاط الذهني الذي يقوم به للوصول إلى الحقيقة، وعليه عرف الاقتناع اليقيني على أنه:" تلك الحالة الذهنية أو النفسية أو

---

[1]- رشيدة بوكر، المرجع نفسه، ص 497.

ذلك المظهر الذي يوضح وصول القاضي باقتناعه لدرجة اليقين بحقيقة واقعة لم تحدث أمام بصره بصورة عامة"[1].

و عليه فإن مبدأ الاقتناع الشخصي للقاضي الجزائي يتجسد في بناء القاضي قناعته على أي دليل تطمئن له نفسه ويسكن إليه وجدانه دون أن يتقيد بأي قيد سوى ما تقتضيه العدالة ذاتها من قيود، والحرية التي يتمتع بها القاضي الجزائي في تقدير الأدلة التي لم تكن بمحض الصدفة أو لمجرد الاحتكام إلى الضمير، وإنما إرساء هذا المبدأ وتبنيه من طرف العديد من التشريعات كان له أسبابه ومبرراته، والتي تمثل أساسا في صعوبة الإثبات في المادة الجزائية وطبيعة المصالح المحمية قانونـــــــــــــا، و من بين هذه التشريعات المشرع الجزائري من خلال المادة 307 من قانون الإجراءات الجزائية المستوحاة من المادة 353 من القانون الفرنسي[2].

2- نطاق تطبيق مبدأ الاقتناع الشخصي للقاضي:

لقد ثار الخلاف حول المجال الحقيقي لإعمال مبدأ الاقتناع الشخصي للقاضي، هل يقتصر تطبيقه على جهات الحكم وحدها؟، أم يمتد تطبيقه إلى جميع مراحل الدعوى العمومية؟.

فأصحاب الرأي الأول يذهبون إلى أن مبدأ الاقتناع الشخصي للقاضي وجد لأجل تطبيقه أمام المحاكم وحدها دون سواها سواء كانت محكمة الجنايات، محكمة الجنح أو المخالفات، وهو ما

[1]-نضال ياسين الحاج حمو، مبدأ اقتناع القاضي الجنائي(دراسة تحليلية تأصيلية في ضوء التشريع البحريني و المقارن)، مجلة كليـــــة القانـون للعلوم القانونية و السياسية، جامعة مملكة البحرين، ص 482، منشور على الموقع: https://www.iasj.net/iasj?func=fulltext&aId=130753، تاريخ الاطلاع 2020/03/15.

[2]- Article 353 du code procédure pénal dispose que : « Avant que la cour d'assises se retire, le président donne lecture de l'instruction suivante, qui est, en outre, affichée en gros caractères, dans le lieu le plus apparent de la chambre des délibérations :

" Sous réserve de l'exigence de motivation de la décision, la loi ne demande pas compte à chacun des juges et jurés composant la cour d'assises des moyens par lesquels ils se sont convaincus, elle ne leur prescrit pas de règles desquelles ils doivent faire particulièrement dépendre la plénitude et la suffisance d'une preuve ; elle leur prescrit de s'interroger eux-mêmes dans le silence et le recueillement et de chercher, dans la sincérité de leur conscience, quelle impression ont faite, sur leur raison, les preuves rapportées contre l'accusé, et les moyens de sa défense. La loi ne leur fait que cette seule question, qui renferme toute la mesure de leurs devoirs : " Avez-vous une intime conviction? ».

ذهب إليه المشرع الفرنسي إذ فصل في المسألة وتناول تطبيق المبدأ أمام محكمة الجنايات حسب أحكام المادة 1/353 من قانون الإجراءات الجزائية، أما المادة 427 من ذات القانون فقد تناولت تطبيق المبدأ أمام محكمة الجنح، في حين أن المادة 536 من ذات القانون نصت على تطبيق المبدأ أمام محكمة المخالفات.

إلا أن المشرع الجزائري فعلى خلاف المشرع الفرنسي، لم ينص صراحة على تطبيق مبدأ الاقتناع الشخصي للقاضي أمام المحاكم وحدها، لكن بالرجوع لأحكام المادتين 212 و 307 من قانون الإجراءات الجزائية التي اندرجت ضمن الكتاب الثاني تحت عنوان جهات الحكم، كما أن المادة 212 جاءت ضمن الأحكام المشتركة أمام جميع جهات الحكم، في حين نصت المادة 307 تطبيق المبدأ أمام محكمة الجنايات، مما يفيد أن هذا المبدأ يطبق أمام جهات الحكم.

أما القائلين بامتداد تطبيق مبدأ الاقتناع الشخصي للقاضي لجميع مراحل الدعوى العمومية، يرون أن هذا المبدأ وإن كان شرع أصلا لتطبيقه أمام جهات الحكم، فهذا لا يمنع من تطبيقه من طرف قضاة التحقيق والنيابة العامة فهم أيضا يقدرون مدى كفاية الأدلة أو عدم كفايتها للاتهام، دون الخضوع لقواعد معينة ولا رقابة للمحكمة العليا في ذلك، بل يخضعون في ذلك لضمائرهم واقتناعهم الذاتي فحسب[1]، ومع ذلك تبقى مرحلة الحكم هي الميدان الأوسع لتطبيقه باعتبارها جهة الفصل عن طريق تقدير الأدلة القائمة من حيث كفايتها أو عدم كفايتها للحكم بالإدانة.

ب/ قيمة الدليل الرقمي كدليل علمي:

تناول المشرع الفرنسي المخرجات الحاسوبية في المادة الجزائية ضمن الأدلة المتحصل عليها من الآلة أو ما يعرف بالأدلة العلمية، سواء كانت عبارة عن بيانات مكتوبة أو صورا، وبالتالي فهو إقرار منه بصلاحية هذه في الإثبات الجزائي .

وكما سبق الإشارة إليه أن دور الخبراء أصبح فعالا مع ظهور الأدلة الرقمية ونقص الخبرة والمعرفة المعلوماتية لدى القضاة، إلا أن النظام السائد في الإثبات يقيم التوازن بين الإثبات العلمي و الاقتناع القضائي، وعليه فإن القاضي له السلطة التقديرية على الأدلة العلمية، وعليه سوف نعرض لدور الخبير في الدعوى العمومية، ثم تقدير الدليل العلمي من جهة أخرى.

1- دور الخبير في الدعوى العمومية:

[1]- أشرف عبد القادر قنديل، المرجع السابق، ص223.

تعد الخبرة التقنية من أهم مظاهر التعاون القضائي مع ظاهرة تكنولوجيا المعلومات والأنترنت التي تقع في اختصاص آخر غير الجوانب النظرية التي لا تسمح ثقافة القاضي المبنية على معايير العدالة والدراسات القانونية من التفاعل معها.

أما عن حجية تقرير الخبير التقني التي تتضمن الأعمال التي قام بها الخبير والنتائج التي توصل إليها تبقى مجرد تقارير استدلالية لأجل إنارة القاضي عملا بأحكام المادة 215 من قانون الإجراءات الجزائية التي تنص على أنه:" لا تعتبر المحاضر والتقارير المثبتة للجنايات والجنح إلا مجرد استدلالات ما لم ينص القانون على خلاف ذلك"، وبالتالي فإن رأي الخبير يعطي على سبيل الاستشارة أين يظل دور القاضي قائما في المفاضلة بين التقارير الفنية الواردة إليه[1].

2- تقدير القضاء للدليل العلمي:

يخضع الدليل العلمي ومنه الدليل الرقمي إلى السلطة التقديرية لقاضي الموضوع، و بالتالي لاقتناعه، وفي هذا الخصوص ينبغي أن نميز بين أمرين: القيمة العلمية القاطعة للدليل الرقمي، وكذا الظروف و الملابسات التي وجد فيها الدليل.

ثانيا/ مدى تأثير مشكلات الدليل الرقمي على إقتناع القاضي:

يثير الدليل الرقمي العديد من المشكلات، التي ترتبط إما بطبيعـــــــــــــــــــــــــــــــه التكوينيـــــــــــــــــــــة من جهـــــــــــــــــــة أو بإجراءات الحصول عليه من جهة أخرى، وهذه المشكلات تؤثر على قيمة الدليل الرقمي في الإثبات إذ تؤدي إلى ضعفه إذا لم يتم إيجاد حلول بشأنها.

أ/ المشكلات الموضوعية للدليل الرقمي:

هناك من الخصائص الفزيائية المكونة للدليل الرقمي ما يثير مشكلات في الإثبات الجزائي، إما بسبب الطبيعة غير المرئية له، أو بسبب مشكلة الأصالة، أو بسبب ديناميكيته.

1- الدليل الرقمي دليل غير مرئي:

الدليل الرقمي عبارة عن سجل كهرومغناطيسي مخزن بنظام حاسوبي في شكل ثنائي وبطريقة غير منظمة لا يدركها الرجل العادي بحواسه الطبيعية، و هذا ما قد يؤدي إلى اختلاط بين الملفات البريئة مع تلك المحرمة والتي تعد موضوعا للدليل الرقمي، مما تؤدي إلى خلق مشكلة التعدي على الخصوصية[2].

---

[1]- رشيدة بوكر، المرجع السابق، ص429.

[2]- أشرف عبد القادر قنديل، المرجع السابق، ص227.

ونذكر أيضا من الأمثلة ملفات الولوج log file التي تشبه الملفات العادية، ويمكن جمعها مثل أي ملف آخر وهي تحتوي على معلومات هائلة قد تفيد في التحقيق، كما أنها قد تختلط بغيرها من المعلومات الخاصة بمستخدمي الكمبيوتر الأبرياء، مما يشكل تهديدا لخصوصية هؤلاء[1].

2- مشكلة الأصالة في الدليل الرقمي:

أسلفنا القول أن الأصالة في الدليل الرقمي لها طابع افتراضي لايرق إلى مستوى الأصالة في الدليل المادي، إلا أن التشريع المقارن اعتمد منطق افتراض الأصالة في الدليل التقني ومنها التشريع الأمريكي الذي نص صراحة على قبول الدليل التقني كمستند أصلي ما دام أن البيانات الصادرة من جهاز الحاسوب أو أي جهاز مماثل أو كانت مطبوعة أو مسجلة على دعامات أخرى ومقروءة للعين المجردة وتعبر عن البيانات الأصلية بشكل دقيق[2].

3- الدليل الرقمي ذو طبيعة ديناميكية:

إن الطبيعة الديناميكية للدليل الرقمي تجعله ينتقل عبر شبكات الاتصال بسرعة فائقة، بمعنى إمكانية تخزين المعلومات في الخارج بواسطة شبكة الاتصال عن بعد، مما يترتب عليه صعوبة تعقب الأدلة الرقمية وضبطها، لأنه يستلزم القيام بأعمال إجرائية على إقليم دولة أخرى مثل تفتيش الأنظمة المعلوماتية عن بعد الذي يتطلب إذن من الدولة المطلوب القيام بالإجراء على إقليمها، أو إبرام اتفاقيات ومعاهدات دولية ثنائية أو متعددة الأطراف في مجال التعاون الدولي.

ب/ المشكلات الإجرائية للدليل الرقمي:

لا تقتصر مشكلات الدليل الرقمي على طبيعته التكوينية، بل تمتد لتشمل الإجراءات المتخذة لأجل الحصول عليه، وتتمثل المشكلات الإجرائية في مايلي:

1- إرتفاع تكاليف الحصول على الدليل الرقمي:

إن نقص المعرفة الفنية و التقنية لرجال القانون يجعل ضرورة اللجوء إلى الخبرة قائمة خاصة في مجال المعلوماتية، إلا أن هذه الخبرة تتطلب مصاريف معتبرة لأجل الحصول على الدليـــــــــــل الرقمي. و لأجل التخفيف من قيمة هذه التكاليف أصبح اللجوء إلى الدورات التدريبية ضروري من خلال تحديد الأساليب التي تساعد في اكتساب الخبرة اتجاه هذه التقنية الحديثة.

2- نقص المعرفة التقنية لدى رجال العدالة:

[1]- رشيدة بوكر ، المرجع السابق، ص456.

[2]- أشرف عبد القادر قنديل، المرجع السابق، ص227.

إن الطبيعة الخاصة للدليل الرقمي باعتباره وسيلة إثبات الجريمة المعلوماتية تتطلب وجود جهات تحقيق ومحاكمة على مستوى من المهارة التي تساعدهم على مواجهة تقنيات الحاسب الآلي وشبكاته، و هو ما سعت إليه الدول سواء على المستوى الداخلي أو الدولي من خلال إنشاء هيئات توكل لها مهمة ضبط هذا النوع من الجرائم و تقديم الدليل بشأنه.

الفرع الثاني

الضوابط التي تحكم اقتناع القاضي الجزائي بالدليل الرقمي:

ترك المشرع للقاضي سلطة واسعة في تقدير الأدلة بما فيها الدليل الرقمي، فله أن يبحث عن الحقيقة وفق كافة الأدلة دون الالتزام المسبق بدليل معين حتى وإن كان هذا الدليل دليلا علميا يقوم على الموضوعية والكفاءة والحياد كما هو الحال بالنسبة للدليل الرقمي، ماعدا الحالات التي ينص عليها القانون بنص خاص، و بالتالي ماهي الضوابط التي تحكم القاضي في تقديره للأدلة من أجل الوصول إلى الاقتناع الشخصي؟، وللإجابة عن هذا التساؤل يتم تقسيم هذه الضوابط إلى ضوابط متعلقة بمصدر الاقتناع وضوابط متعلقة بالاقتناع ذاته.

أولا/ الضوابط المتعلقة بمصدر الاقتناع:

سبق القول أن القاضي الجزائي لا يمكن أن يبني اقتناعه إلا على الدليل المقبول، أي تم الحصول عليه بالطريق المشروع، وتمت مناقشته حضوريا أمامه وهو ما يعرف بوضعية الدليل.

1- مشروعية الدليل الرقمي:

تعد مشروعية الدليل الرقمي ضمانة كبيرة للحرية الفردية وللعدالة ذاتها، كما أنها تحمل القائمين على تجميع أدلة الإدانة للقيام بعملهم بكل نزاهة، فليست الغاية هي الإدانة وإنما هي تحقيق العدالة، ولا يمكن لمبدأ قرينة البراءة أن يهدم إلا بناء على أدلة صحيحة مشروعة[1].

وعليه يكون الدليل الرقمي موضع شك من ناحيتين[2]:

الناحية الأولى: تمثل في إمكانية العبث بالدليل التقني، و بالتالي الخروج به على نحو يخالف الحقيقة الذي لا يمكن إدراكه إلا من قبل المختصين في هذا المجال.

أما الناحية الثانية: تجلى في إمكانية الخطأ في الحصول على الدليل الرقمي، بالرغم من أن نسبة الخطأ نادرة، و يتحقق الخطأ بالنسبة للدليل الرقمي في سببين

[1]- أشرف عبد القادر قنديل، المرجع نفسه، ص253.

[2]- ميسون خلف حمد الحمداني ، المرجع السابق، ص242-243.

1- الخطأ في استخدام الأداة المناسبة في الحصول على الدليل الرقمي، ويرجع ذلك لخلل في الشفرة المستخدمة أو بسبب استخدام مواصفات خاطئة.

2- الخطأ في استخلاص الدليل، ويكون سببه استخدام أداة نسبة صوابها تقل عن 100% ويحدث هذا في أغلب الأحيان بسبب وسائل اختزال المعطيات، أو بسبب معالجة المعطيات بطريقة تختلف عن الطريقة الأصلية التي تم تقييمها.

ويتم التحقق من سلامة الدليل الرقمي سواء من حيث العبث به أو من حيث سلامة الاجراءات الفنية للحصول عليه على النحو التالي:

أ/ تقييم الدليل الرقمي من حيث سلامة العبث به:

يمكن التأكد من سلامة الدليل الرقمي من العبث بعدة طرق نذكر منها[1]:

1- يمكن الاستعانة بعلم الكمبيوتر في كشف مدى التلاعب بمضمون هذا الدليل، وتبدو فكرة التحليل التناظري الرقمي من الوسائل المهمة للكشف عن مصداقية الدليل الرقمي، ومن خلالها يتم مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بالآلة الرقمية.

2- كما يمكن استخدام عمليات حسابية خاصة تعرف بالخوارزميات إذ يتم من خلالها الكشف عن وجود تلاعب حتى في النسخة الأصلية.

3- استخدام الدليل المحايد وهو دليل لا علاقة له بموضوع الجريمة، ولكن يساعد في الكشف ما إذا كان هناك تلاعب أو تغيير في النظام الكمبيوتري.

ب/ تقييم الدليل الرقمي من حيث سلامة وصحة إجراءات الحصول عليه:

قد يعتري الإجراءات الفنية للحصول على الدليل الرقمي أخطاء تؤدي إلى التشكيك في النتائج التي تم التوصل إليها، لذا سنعرض للخطوات المتبعة لأجل التأكد من سلامة هذه الإجراءات فنيا[2].

ب-1/ إخضاع الأداة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج المرجوة بإتباع اختبارين رئيسيين هما:

أ/ اختبار السلبيات الزائفة، ويفيد هذا الاختبار إخضاع الأداة المستخدمة في الحصول على الدليل الرقمي لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الرقمي دون إغفال لمعطيات مهمة عنه.

1- رشيدة بوكر، المرجع السابق، ص500.

2- رشيدة بوكر، المرجع نفسه، ص501.

ب/ اختبار الإيجابيات الزائفة، ويكون هذا الاختبار في اخضاع أداة الحصول على الدليل الرقمي لاختبار فني يؤكد عدم عرض الأداة لمعطيات إضافية جديدة.

ب-2/ الاعتماد على الأدوات التي أثبتت البحوث العلمية كفاءتها في تقديم نتائج أفضل:

أشارت البحوث المستمرة في مجال تقنية المعلومات على الطرق السليمة الواجب اتباعها للحصول على الأدلة الرقمية، كما بينت الأدوات التي تؤدي إلى التشكيك في مصداقية المخرجات المستمدة منها.

2- وضعية الدليل الرقمي:

أقرت المادة 212 من قانون الإجراءات الجزائية صراحة على أنه لا يمكن للقاضي أن يبني حكمه إلا على الأدلة المقدمة له في معرض المرافعات والتي تمت مناقشتها حضوريا أمامه، وهو ما يعبر عنه بوضعية الدليل، ومقتضى ذلك أن يكون للدليل أصل ثابت في أوراق الدعوى، وأن يعرض على الخصوم لأجل مناقشته، لأنه لا يجوز للقاضي أن يقضي اعتمادا على معلوماته الشخصية أو رأي غيره.

فالقاضي لا يكتفي بما دون في محاضر التحقيق، بل من واجبه إعادة سماع الشهود الذين سبق سماعهم في محاضر التحقيق الابتدائي، وكذلك مناقشة تقارير الخبراء التي خلصوا إليها لإظهار الحقيقة، وقد أكدت المحكمة العليا هذا الضابط في العديد من قراراتها، وهذا ما ينطبق أيضا على الدليل الرقمي.

2*النتائج المترتبة على وضعية الدليل الرقمي:

تترتب على وضعية الدليل الرقمي نتائج يجب على القاضي أخذها بعين الاعتبار و التي تتمثل في عدم امكانية اعتماد القاضي في بناء حكمه على معلوماتـه الشخصيـة أو رأي غيره، كما أنه يتوجب أن يتمتع القاضي بتأهيل تقني يساعده في فهم الدليل الرقمي ومناقشته.

*** عدم جواز قضاء القاضي استنادا على معلوماته الشخصية أو رأي غيره:**

يقصد بالعلم الشخصي للقاضي معلوماته الشخصية التي يكون قد حصل عليها من خارج مجلس القضاء ونطاق الدعوى المطروحة عليه، والتي من الممكن أن تؤثر في تكوين قناعته عند تقديره لأدلتها[1].

---

[1]- محمد حسين، الحمداني، نوفل علي الصفو ، مبدأ الاقتناع القضائي، المجلد1، العدد 24، السنة العشرة، مجلة الرافدين للحقوق، جامعة الموصل، 2005 ص256، منشور على الموقع: http://rights.uomosul.edu.iq/files/files/files_2735859.pdf، تاريخ الاطلاع: 2020/03/15.

والعلة في استبعاد بناء القاضي اقتناعه على معلوماته الشخصية تكمن:

أولا: في أنها لم تكن موضع مناقشة شفاهية بين أطراف الدعوى حتى يتمكنوا من الرد عليها، وبالتالي ستكون مفاجأة بالنسبة لهم لأنه لم يتم إثباتها في إطار إجراءات الخصومة، مما يؤدي إلى عدم احترام حقوق الدفاع و إساءة الظن بالقاضي وهو الشيء الذي يجب أن ينزه عنه القضاء عموما[1].

ثانيا: جمع القاضي لصفتين متعارضتين وهي صفة الشاهد وصفة القاضي خاصة أن الشهادة لا تقبل إلا بعد حلف اليمين، وهذا لا يجيزه القانون ويترتب عليه بطلان الحكم[2].

والجدير بالذكر هنا أن المعلومات التي يستقيها القاضي من خبرته بالشؤون العامة التي يفترض فيه الالمام بها، لا تعد من قبيل المعلومات الشخصية التي يحظر على القاضي بناء حكمه عليها، ومن قبيل ذلك الثقافة المعلوماتية كالمعرفة بمبادئ الكمبيوتر ومكوناته[3]، ليست من المعلومات الشخصية التي يمنع على القاضي اعتمادها في بناء حكمه.

والقول بما سبق لا يتعارض مع الجهود التي يقوم بها القاضي للبحث عن الحقيقة التي تماشى والدور الايجابي الذي يلعبه القاضي الجزائي، طالما أن ما توصل إليه يتم عرضه للمناقشة الشفوية من قبل أطراف الدعوى الجزائية في جلسة المحاكمة.

كما يشترط لسلامة الحكم عدم الاعتماد على رأي الغير وليس مفاد ذلك حرمان القاضي بصفة مطلقة في الأخذ برأي الغير، إذ يجوز للقاضي إذا كان الغير من الخبراء الاستناد إلى تقاريرهم متى ارتاح لها ضميره من بين الأدلة الموجودة بملف الدعوى المعروضة على القاضي للفصل فيها، وبالتالي يكون اقتناع القاضي في إصدار حكمه مبنيا على عقيدته هو وليس تقرير الخبير[4].

*** ضرورة التأهيل التقني والفني للقضاة:**

يشترط مجال الأدلة الرقمية أن يكون القاضي الجزائي مؤهلا تقنيا وفنيا تأهيلا كافيا لكيفية التعامل مع الدليل الرقمي الذي سيتم عرضه للمناقشة الشفوية الحضورية من قبل الأطراف، فحتى ينجح القاضي في مهمته والوصول إلى الحقيقة لابد أن تكون له الدراية الكافية لأجل المناقشة

---

[1]- رشيدة بوكر، المرجع السابق، ص514.

[2]-محمد حسين الحمداني ، نوفل علي الصفو ، المرجع السابق، ص256.

[3]- أشرف عبد القادر قنديل، المرجع السابق، ص240.

[4]- رشيدة بوكر، المرجع السابق، ص515.

العلمية والسيطرة على الدعوى الجزائية، و لا يتحقق هذا الأمر إلا عن طريق إعداد دورات تكوينية للقضاة في مجال تقنية المعلومات.

ثانيا/ الضوابط المتعلقة بالاقتناع ذاته:

يفيد مبدأ الاقتناع الشخصي للقاضي الذي تبناه المشرع الجزائري طبقا لأحكام المادة 212 من قانون الإجراءات الجزائية، إعطاء حرية واسعة للقاضي في تقدير عناصر الإثبات بما فيها الدليل الرقمي وهذا لأجل الوصول إلى الحقيقة الواقعية اليقينية، كما أن حرية القاضي الجزائي في الاقتناع هي أمر موضوعي يدخل في نطاق السلطان النهائي لقاضي الموضوع.

وترتيبا على ذلك فإن تكوين القاضي لقناعته وعقيدته يقوم على شرطين أساسيين هما بلوغ الاقتناع القضائي درجة اليقين و بناء القاضي لاقتناعه على الأدلة مجتمعة دون أن يكون هناك تناقض أو تخاذل فيما بينها.

أ/ بلوغ الاقتناع القضائي درجة اليقين:

تصبو الخصومة الجزائية إلى معرفة الحقيقة، وحتى يتمكن القاضي من الوصول إلى هذه الحقيقة وإصدار حكمه لا بد أن يتوفر لديه اليقين، واليقين عبارة عن حالة ذهنية وعقلية تؤكد وجود الحقيقة، أو هو اعتقاد القاضي بأن ما وصل إليه هو الحقيقة[1].

ويتم الوصول إلى اليقين عن طريق نوعين من المعرفة أولهما المعرفة الحسية التي تدركها الحواس، وثانيهما المعرفة العقلية التي يقوم بها القاضي عن طريق التحليل والاستنتاج، واليقين الذي يلزم القاضي الوصول إليه لأجل بناء اقتناعه هو اليقين القضائي وليس اليقين الشخصي.

و عليه يثور التساؤل هل يمكن إعمال الحواس والاستنتاجات في جريمة تعتمد على التقنية الحديثة والهندسة الرقمية؟. للإجابة عن هذا التساؤل يستوجب أولا التطرق لتحديد المقصود باليقين القضائي وثانيا تفسير الشك لمصلحة المتهم.

1/ اليقين القضائي:

يقصد به اليقين الذي يتطلبه القاضي الجزائي في بناء اقتناعه بالنسبة للجرائم المعلوماتية، وهو ذات اليقين الذي يشترط في الجرائم التقليدية لأجل الحكم بالإدانة[2]، ويقوم على وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من أدلة رقمية يستطيع القاضي من خلالها وما ينطبع

1- نضال ياسين الحاج حمو ، المرجع السابق، ص522.

2- هلالي عبد اللاه أحمد، المرجع السابق، ص190.

في ذهنه من تصورات واحتمالات بالنسبة لها أن يحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه.

إلا أن نقص المعرفة بالعلوم التقنية وما تقوم عليه من معادلات حسابية لدى القاضي الجزائي تجعله يجهل بكل ما يدور حول الجريمة المعلوماتية، وبالتالي يصعب على القاضي وضع استنتاجات من أشياء يجهلها، فالقاضي مثلا ليس له علم ومعرفة بما وصل إليه العلم فيما يتعلق بالبرامج التخريبية والفيروسات إلى غير ذلك من التطورات التقنية في مجال المعلوماتية، و هو ما يجعله في حقيقة الأمر عاجزا عن الوصول إلى اليقين الذي يشترط في بناء اقتناعه أو التشكيك في الدليل مما يؤدي إلى الحكم بالبراءة، وعليه فإن المعرفة الحسية والعقلية التي يعتمدها القاضي في الوصول باقتناعه إلى اليقين والجزم غير كافية في الجرائم المعلوماتية، بل لا بد من توافر المعرفة العلمية التقنية في مجال المعلوماتية، مما يؤكد ضرورة وأهمية تدريب وتكوين القضاة في المجال المعلوماتي.

2/ قاعدة الشك يفسر لمصلحة المتهم:

تعد هذه القاعدة من النتائج المترتبة عن قرينة البراءة، والتي مفادها أن القاضي الجزائي لا يطمئن لثبوت التهمة ونسبتها إلى المتهم، مما يجعله ملزم بإصدار حكم البراءة .

وتطبق قاعدة الشك يفسر لمصلحة المتهم في مرحلة المحاكمة دون باقي مراحل الدعوى العمومية الأخرى، و المشرع الجزائري لم يوضح موقفه من هذه القاعدة، و لا كيفية إعمالها في المجال القضائي، إلا أن الاجتهاد القضائي أكد على هذه القاعدة في العديد من قراراته.

والجدير بالذكر أن الإشكال الذي ما زال قائما هو الحالات التي يثور فيها الشك، وقد انقسم الفقه بشأن هذه المسألة إلى اتجاهين[1]:

الاتجاه الأول: يتزعمه الفقيه الفرنسي "فوان"، ويذهب أنصاره إلى أن قاعدة الشك يفسر لمصلحة المتهم تقتصر على الحالات التي يكون فيها الشك موضوعيا، أي يتعلق بماديات الواقعة الإجرامية.

الاتجاه الثاني: يذهب أصحاب هذا الاتجاه إلى أن قاعدة الشك يفسر لمصلحة المتهم تنطبق على كافة الحالات التي يوجد فيها شك في إدانة المتهم، سواء كان هذا الشك موضوعيا، أو شخصيا يتعلق بتقدير القاضي لقيمة الأدلة المطروحة أمامه.

ويذهب أغلب الفقه إلى تبني الاتجاه الثاني، لأن اقتصار القاعدة على الشق الموضوعي فيه تقييد لمبدأ حرية القاضي في الاقتناع، لأن اليقين يقوم على عنصرين أحدهما شخصي يتمثل في ارتياح

[1]- أشرف عبد القادر قنديل، المرجع السابق، ص242.

ضمير القاضي و اطمئنان نفسه إلى إدانة المتهم على سبيل الجزم واليقين، والثاني موضوعي يخص ارتكان هذا الارتياح و الاطمئنان على أدلة من شأنها أن تفضي لذلك وفقا لمقتضيات العقل والمنطق.

ب/ بناء الاقتناع من الأدلة مجتمعة دون تناقض أو تخاذل فيما بينها:

حتى يكون اقتناع القاضي الجزائي صحيحا يجب أن تكون الأدلة التي يعتمدها متماسكة ومتساندة ومتكاملة فيما بينها و غير مبهمة وغامضة، فيتكون اقتناع القاضي منها مجتمعة دون تناقض أو تخاذل إذ تؤدي وفق قواعد العقل والمنطق السليم إلى الحكم الصحيح، و لأجل التوضيح أكثر نعرض لمايلي:

1/ انعدام الغموض و الإبهام:

يقصد به التزام القاضي بتسبيب حكمه بصفة واضحة أي بيان الأدلة المستند إليها دون إبهـــــــــــام أو غموض، فلا يقتصر الإشارة إلى الأدلة المعتمدة في إدانة المتهم، بل لا بد أن يحدد مضمون الدليل، وهذا حتى تتمكن المحكمة العليا من بسط رقابتها على الوجه الصحيح، إذ أن رقابة المحكمة العليا لا تكون مجدية إلا إذا كانت الأحكام مسببة تسبيبا كافيا وواضحا.

وترتيبا على ذلك فإنه يستوجب على القاضي تحديد مضمون الأدلة الرقمية المعتمد عليها للوصول إلى الاقتناع الشخصي، وإلا سيشوبها الغموض والإبهام، مما يجعل من تأهيل القاضي في مجال التقنية الحديثة ضرورة ملحة حتى يتمكن من تسبيب أحكامه تسبيبا كافيا ومنطقيا في اللجوء والاعتماد على الأدلة الرقمية.

2/ انعدام التناقض والتخاذل:

يتحقق التناقض الذي ينفي الاقتناع الشخصي للقاضي الجزائي، إما بتناقض الأدلة فيما بينها بالنسبة للجريمة المعلوماتية، أو في التناقض الذي يحصل بين أدلة الإثبات ومنطوق الحكم.

ومن أمثلة التناقض بين الأدلة وجود دليلين أحدهما قولي والآخر فني فيقوم القاضي باعتمادها معا في إصدار حكمه، أي أن القاضي يعتمد في بناء اقتناعه وتكوين عقيدته على شهادة الشاهد الوحيد الذي يؤكد أن الاعتداء الحاصل على المعلومات عن طريق ارسال فيروس قد تم بواسطة حاسب آلـــــي معين، في حين أن تقرير الخبير يؤكد أن ذات الاعتداء الحاصل على المعلومات تم بواسطة حاسب آلي آخر غير الذي ذكره الشاهد، كما أن القاضي لم يفسر التناقض في الجمع بين الدليلين المتناقضين حتى يتمكن العقل من تقبل هذا الجمع.

أما التناقض الحاصل بين أدلة الإثبات ومنطوق الحكم فمن صوره أن يفهم من تسبيب الحكم عدم ثبوت الواقعة ثم ينتهي في منطوق الحكم إلى الإدانة أو بالعكس، وهو ما أكدته المحكمة العليا في العديد من قراراتها أين يستلزم القانون أن تكون الأسباب أساسا للحكم، ويترتب على هذه القاعدة أنه لا يجوز للقاضي أن يورد في حكمه أو قراره أسبابا للإدانة ثم ينطق بالبراءة، أو يستدل بأسباب البراءة ثم ينطق بالإدانة، فالتناقض بين الأسباب والمنطوق يؤدي دائما إلى البطلان والنقض[1].

الخاتمة:

إن التقدم العلمي في مجال التقنية الحديثة لم يكن له الأثر فقط على استحداث نوع جديد من الجرائم و المجرمين، و إنما أدى إلى ظهور أدلة جديدة تعرف بالأدلة الرقمية التي تختلف من حيث خصائصها و طبيعتها عن الدليل المادي الذي ألف المحققون و رجال القضاء التعامل معه، و عليه فإن الطبيعة الفنية المعقدة للدليل الرقمي أثارت صعوبة فهمه بصورة واضحة و جلية من طرف رجال القضاء مما أقام ضرورة الاستعانة بأهل الاختصاص في العالم الافتراضي.

كما أن العديد من التشريعات الوطنية لم تنص صراحة على مخرجات الحاسب الآلي كدليل أمام القضاء و هو ما جعل الدراسة الحالية تعتمد بصفة أكثر على الاتجاهات الفقهية بدلا من تحليل التشريعات القائمة الذي اقتصر على اسقاط النصوص المنظمة للدليل المادي على الدليل الرقمي، وعلى ضوء ذلك تم التوصل إلى النتائج و الاقتراحات التالية:

النتائج :

1- منح المشرع الجزائري دورا ايجابيا للقاضي الجزائي في قبول الدليل وتقدير قيمته الإثباتية على غرار القوانين ذات الصياغة اللاتينية منها المشرع الفرنسي، وهو ذات الحكم الذي طبق على الدليل الرقمي إذ لم يتضمن القانون 09- 04 أي أوضاع خاصة بهذا الصدد.

2- حرصت كافة التشريعات المختلفة ومنها المشرع الجزائري على تطبيق مبدأ مشروعية الدليل الرقمي.

---

[1]- ايمان محمد علي الجابري، يقين القاضي الجنائي(دراسة مقارنة)، دار منشأة المعارف، الاسكندرية،2005، ص352.

3- الانتهاء إلى الحقيقة العلمية قد تشوش وتضلل الحقيقة القضائية، وهو ما يلقي مزيدا من الأهمية لتدريب المحققين والقضاة لأجل فهم هذه الحقيقة العلمية والعمل على مطابقة الحقيقة القضائية لها على قدر المستطاع.

4- الدليل الرقمي ذو طبيعة غير مرئية يصعب الحصول عليه، إلا أن التطور التقني أوجد من البرامج ما يمكن استرجاعه حتى في حالة محوه.

الاقتراحات:

1- وجوب الأخذ بعين الاعتبار مبدأ افتراض الدليل الرقمي كدليل أصلي وذلك نتيجة نقص توافر الإمكانيات الرقمية في المحاكم.

2- حبذا لو يتدخل المشرع الجزائري لأجل تنظيم الدليل الرقمي خاصة من حيث حجيته و طرق الحصول عليه.

3- العمل على تدريب المحققين و حتى قضاة الحكم على كيفية التعامل وفهم الدليل الرقمي للحد من ظاهرة الإجرام المعلوماتي.

إشكالية الاختصاص في الجريمة الإلكترونية

The problem of jurisdiction in electronic crime

د. حماس عمر أستاذ محاضر –ب-
معهد الحقوق و العلوم السياسية
المركز الجامعي بمغنية - الجزائر

مقدمة :

تميز القرن الماضي باختراعات هائلة من ظهور واستعمال الكمبيوتر واستحداث شبكات الإنترنت التي يسرت سبل التواصل وانتقال حركة المعلومات بين مختلف الشعوب إذ أصبح يسمى بقرن المعلوماتية ، إلا أنّ هذا التقدم المذهل والمميز أسفر على ظهور أشكال إجرامية جديدة والمتمثلة في جرائم الإنترنت أو جرائم المعلوماتية .

ومع تزايد معدلات هذه الجرائم وتطور أشكالها استوجب تضافر وتكاتف الجهود سواء كانت وطنية أو دولية من أجل وضع حد لها .

ولقد أفرزت الجريمة الالكترونية تحديات واضحة للقوانين الوضعية التي وضعت لمكافحتها ، بسبب تقنيتها العالية وصارت أكثر قوة بفضل التقنية الحديثة .

وما يرجع الأمر تعقيدا أنّ هذه الجريمة عالمية بمعنى أنها تعدت الحدود الجغرافية للدول أي أصبحت عابرة للقارات ، لأنه مع انتشار شبكة الإتصالات العالمية والإنترنت أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة ، لذلك تطرح هذه الجرائم مشاكل قانونية خصوصا في مجال الاختصاص من حيث الجهات المخول لها متابعة المجرم ، أو من خلال المحكمة المختصة فقد ترتكب الجريمة في دولة و تكون آثارها في دولة أخرى ، وقد يكون الجاني يحمل جنسية دولة وتكون أدلة الجريمة موجودة في دولة أخرى وخارج النطاق الإقليمي لجهة التحقيق، وهذا ما يحتم علينا ضرورة البحث عن الاختصاص في جرائم المعلوماتية العابرة للحدود على المستوى الداخلي .

فالإشكالية المطروحة في هذا الشأن هي كالآتي : **ما هو القانون الواجب التطبيق على الجريمة الإلكترونية ؟ وإلى أي مدى يمكن تطبيق القانون الوطني عليها ؟**

وللإجابة على هذا التساؤل ارتأينا تقسيم هذا البحث إلى المطلبين التاليين :

المطلب الأول : مبدأ إقليمية الجريمة الإلكترونية

المطلب الثاني : الإستثناءات الواردة على مبدأ إقليمية الجريمة الإلكترونية

المطلب الأول : مبدأ إقليمية الجريمة الإلكترونية

قبل التطرق إلى هذا المبدأ ، لا بأس أن نمنح تعريفا للجريمة الإلكترونية إذ أنّه لا يوجد تعريف موحد ومتفق عليه ، فهناك من عرفها على أنّها : " تلك التي يكون محلها المعطيات المعالجة بلغة الآلة أي المعلومات والبرامج ، أو بمفهوم أوسع النظام المعلوماتي " [1] ، وهناك من منحها تعريفا آخر وهو : " مجموعة الأفعال التي تستهدف معلومات محمية قانونا ، بواسطة التقنية المعلوماتية لتحقيق غرض غير مشروع " [2] فهي إذن كل فعل أو إمتناع عمدي ينشأ عن الإستخدام غير المشروع لتقنية المعلومات ويهدف إلى الإعتداء على الأموال المادية والمعنوية [3] ومهما تنوعت وتعددت التعاريف الخاصة بهذه الجريمة فقد أجمع العالم بأسره على خطورتها ، لذلك كان لزاما على كل دولة إعداد قوانين فعالة لمكافحتها وتطبيقها على مجرمي الأنترنت ، وهذا لا يطرح أي إشكال كمبدأ عام عندما ترتكب الجريمة داخل أراضيها. وسنحاول في هذا المطلب التطرق إلى تعريف مبدأ إقليمية الجريمة الإلكترونية (الفرع الأول) ، وتطبيقاته في كل من التشريع الجزائري وبعض التشريعات الأجنبية (الفرع الثاني) .

الفرع الأول : تعريف مبدأ إقليمية الجريمة الإلكترونية

تعتبر الجرائم الإلكترونية من بين الجرائم التي تثير مسألة الإختصاص القضائي وهذا نظرا لعالميتها، حيث توصف بالجريمة العابرة للحدود (la criminalité transnationale) إذ أنّها ترتكب في أكثر من دولة[4] لذلك تحتاج إلى تعاون دولي شامل يهدف إلى مكافحتها مع احترام السيادة الوطنية للدول المعنية [5] .

---

[1]- غنية باطلي ، الجريمة الإلكترونية دراسة مقارنة ، منشورات الدار الجزائرية ، الجزائر ، 2016 ، ص.24 .

[2] بن مكي نجاة ، السياسة الجنائية لمكافحة جرائم المعلوماتية ، دار الخلدونية ، الجزائر ، 2017 ، ص.15 .

[3] منار عبد المحسن عبد الغني وآخرون ، المواجهة القانونية لجرائم الأنترنت بين مبدأ المشروعية وقصور التشريع ودور القضاء في معالجته ، مجلة الجامعة العراقية ، مركز الدراسات والبحوث الإسلامية ، المجلد 39 ، العراق ، 2017 ، العدد 2 ، ص.429 .

[4] Papa Gueye , Criminalité organisée , terrorisme et cybercriminalité : réponses de politiques criminelles , L'Harmattan , Sénégal , 2018 , P.25 .

[5] معتز سيد محمد أحمد عفيفي ، قواعد الإختصاص القضائي بالمسؤولية الإلكترونية عبر شبكة الأنترنت ، الطبعة الأولى ، دار الجامعة الجديدة للنشر ، الإسكندرية ، مصر ، 2013 ، ص.33 .

وبالرجوع إلى التشريع الجزائري نجد أنّ قانون العقوبات يعدّ مظهرا من مظاهر السيادة ويحكم التشريع العقابي ما يسمى بمبدأ إقليمية النص الجنائي والذي يؤدي إلى إخضاع الجرائم المرتكبة على إقليم الدولة لقانونها أيا كانت جنسية الفاعل[1]، وهذا ما كرسته المادة 3 من قانون العقوبات الجزائري التي نصت على ما يلي: " يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية الجزائرية " [2] .

واستنادا لهذا المبدأ يجب على القاضي الجنائي تطبيق القانون الوطني سواءا في شقه الموضوعي أو في جانبه الإجرائي ، فلا يجوز للأجنبي أن يتمسك بالإجراءات المطبقة في دولته ، بل يخضع لإجراءات قانون الدولة المرتكب على إقليمها[3].

فبدأ الإقليمية هو تطبيق قانون الدولة التي ارتكبت على إقليمها وداخل حدودها ونفاذ سلطان قضائها في متابعة ومحاكمة مرتكب الجريمة الإلكترونية بغض النظر عن جنسية الجاني أو المجني عليه ، أو نوع الجريمة المرتكبة وطبيعتها ، كما لا يؤخذ بعين الإعتبار بالمصالح التي تعرضت للإعتداء .

إلاّ أنّ المشكل المطروح في هذا الصدد هو أنّ تطبيق مبدأ الإقليمية قد يثير فكرة تنازع الإختصاص القضائي ، لذلك سنحاول توضيح موقف كل من التشريع الجزائري وبعض التشريعات الأجنبية من تطبيقه (الفرع الثاني) .

الفرع الثاني : تطبيقات مبدأ إقليمية الجريمة الإلكترونية

كما سبق القول هو أنّ تطبيق هذا المبدأ قد يثير مسألة تنازع الإختصاص القضائي ، فلو قام الجاني من إقليم دولة معينة باختراق مواقع إلكترونية لمؤسسات أجنبية ويتمكن من خلالها من سحب أموال معتبرة ، وبالرجوع إلى القانون رقم 09-04 [4] يتضح أنّه في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المنصوص عليها في هذا القانون والكشف عن مرتكبيها ، فإنّ السلطات الجزائية المختصة بإمكانها تبادل المساعدة القضائية الدولية لجمع الأدلة

[1] حمزة خشاب تحت إشراف مولود ديدان ، مدخل إلى العلوم القانونية ونظرية الحق ، دار بلقيس ، الجزائر ، 2014 ، ص.114 .

[2] المادة 3 من الأمر رقم 66-156 المؤرخ في 8 جوان 1966 والمتضمن قانون العقوبات الجزائري ، جريدة رسمية مؤرخة في 11 جوان 1966 ، العدد49

[3] حمزة خشاب تحت إشراف مولود ديدان ، نفس المرجع ، ص.114 .

[4] قانون رقم 09-04 المؤرخ في 5 أوت 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، جريدة رسمية مؤرخة في 16 أوت 2009 ، العدد 47 .

الخاصة بالجريمة الإلكترونية ، وتتم هذه المساعدة وفقا للإتفاقيات الدولية ذات الصلة والإتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل ، إضافة إلى ذلك يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام ، كما يجب التقيد بشرط المحافظة على سرية المعلومات المبلغة لتلك الدولة وعدم استعمالها في غير ما هو موضح في طلب المساعدة [1] .

واعتمادا لما سبق ، باشرت السلطات الجزائرية العديد من الأعمال الإجرائية في إطار المساعدة القضائية الدولية واتخذت إزاء ذلك تدابير منها إحالة بعض المتهمين على العدالة ، وهذا منذ دخول القانون رقم 09-04 السابق الذكر حيّز التنفيذ وهي القضايا التي تورط فيها جزائريون وأجانب استهدفت شبكات وقواعد بيانات لمؤسسات جزائرية وأجنبية ، ففي إطار تنفيذ المساعدة القضائية الدولية والإنابة القضائية تمت متابعة شاب جزائري وإحالته على العدالة بمحكمة الجنح بباتنة وهو شاب عمره 21 سنة تقني سامي في الإعلام ، قام باختراق موقع شركة أمريكية متخصصة في حماية المعلومات والبرامج الإلكترونية للعديد من الشركات الأمريكية ثمّ عمل على استغلال تلك المعلومات لصالح شركات منافسة مقابل مبالغ مالية ، وإثر إيداع شكوى من قبل الشركة المتضررة لدى الشرطة الأمريكية قدمت هذه الأخيرة المعلومات الكافية بشأن المتهم المشار له إلى مصالح الأمن الجزائري [2] .

وهناك حالة أخرى تتعلق بمتابعة ومحاكمة شاب جزائري وهو طالب جامعي بقسم الإعلام الآلي بعنابة من طرف سلطات الأمن الجزائري ، والذي تمكن من قرصنة عدد كبير من البطاقات البنكية عقب اختراقه لمواقع إلكترونية لمؤسسات أجنبية في أوربا والولايات المتحدة الأمريكية وفي كندا وتمكن من سحب أموال معتبرة ومن خلال تبادل المعلومات مع الأمن الجزائري في إطار المساعدة القضائية الدولية تمت متابعة البريد الإلكتروني الذي كان يستعمله "الهاكرز" [3] المتهم المشار له والذي حوكم وأدين من طرف محكمة الجنح بعنابة ثم استفاد من تدابير المنفعة

[1] المادة 16 ، 17 و18 من نفس القانون ، ص.8 .

[2] زيحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى للطباعة والنشر والتوزيع ، الجزائر، 2011 ، ص.146-147 .

[3] هو أي شخص يستطيع النفاذ خفية إلى الأنظمة الحاسوبية والعبث بالبرامج والمعلومات المخزنة فيها دون أن يكون مخولا بذلك : أنظر في ذلك : ساري محمد الخالد ، إتجاهات في أمن المعلومات وأمانها ، أهمية تقنيات التعمية (الشفرة) ، الطبعة الأولى ، العبيكان للنشر والتوزيع ، الرياض ، السعودية ، 2018 ، ص.95 .

العامة وفقا لما ورد في الفصل الأول مكرر طبقا للمادة 5 مكرر 1 إلى المادة 5 مكرر 6 من قانون العقوبات الجزائري [1] .

ومن خلال الأمثلة المذكورة سابقا يتضح أنّ المشرع الجزائري قد أخذ بمبدأ الإقليمية واعتبر أنّ القضاء الجنائي الجزائري هو المختص عندما يرتكب عمل من الأعمال المميزة لأحد الأركان المكونة للجريمة الإلكترونية في الجزائر [2] .

نفس الشأن بالنسبة للقانون المصري الذي يعتبر أنّ القضاء الجنائي الوطني هو المختص بالنظر في الجرائم المرتكبة على الأنترنت وفقا للمواد 217 ، 218 ، 219 من قانون الإجراءات الجنائية ، حيث أكدت تلك المواد على اختصاص القاضي الجنائي المصري بنظر الجريمة المرتكبة داخل القطر المصري من مصري أو أجنبي ، واعتدت المادة 218 السالفة الذكر بأحد الأعمال المكونة للركن المادي للجريمة في أي جزء من الإقليم المصري ، أي إذا وقع السلوك الإجرامي أو النتيجة الإجرامية في مصر فمثلا إذا قام مواطن مصري أو أجنبي بسب و قذف مواطن آخر مصري أو أجنبي عبر شبكة الأنترنت من خلال إرساله رسالة عبر البريد الإلكتروني أو من خلال مواقع تويتر (Twitter) أو الفيسبوك (Facebook) ففي هذه الحالة يختص القاضي المصري بنظر جريمة السب والقذف بغض النظر عن جنسية الجاني أو المجني عليه وذلك لأنّ الفعل المجرم وقع داخل الأراضي المصرية .

ومن أشهر القضايا التي تصدت لها المحاكم الجنائية المصرية القضية الشهيرة بالسب والقذف عبر موقع الفيسبوك (قضية أشرف ذكي ضد هشام بهاء الدين) ، وترجع وقائع القضية إلى أنّ السيد هشام بهاء الدين عضو نقابة المهن التمثيلية قام بسب وقذف الدكتور " أشرف زكي " نقيب المهن التمثيلية عن طريق مقال كتبه على الفيسبوك وانتقد فيه أداء مجلس النقابة الحالي ، وعلى إثر ذلك قدمت النيابة المتهم للمحاكمة أمام محكمة جنح العمرانية والتي أصدرت حكمها في 15 ماي 2010 على " هشام " بالحبس لمدة أسبوعين وكفالة 10 جنيهات لإيقاف التنفيذ ، وبعد استئناف الحكم قضت محكمة جنح مستأنف العمرانية ببراءة " هشام بهاء الدين " ، وتعتبر هذه القضية أول

---

[1] زبيحة زيدان ، المرجع السابق ، ص.147 .

[2] المادة 586 من الأمر رقم 66-155 المؤرخ في 8 جوان 1966 ، والمتضمن قانون الإجراءات الجزائية الجزائري ، جريدة رسمية مؤرخة في 10 جوان 1966 ، العدد 48 .

قضية سب وقذف عبر موقع التواصل الإجتماعي الفيسبوك والمحاكم المصرية مختصة بحكم أنّ الجريمة وقعت داخل الأراضي المصرية عبر شبكة الأنترنت [1] .

كما أخذ المشرع الفرنسي بهذا المبدأ طبقا للمادة 113 فقرة 2 من قانون العقوبات الجديد والتي اعتبرت أنّ القانون الفرنسي هو الواجب التطبيق على الجرائم المرتكبة داخل إقليم الجمهورية، وتعدّ الجريمة مرتكبة على إقليم الجمهورية إذا كان أحد عناصر الجريمة قد وقع على هذا الإقليم [2] .

وتجدر الإشارة إلى أنّ مسألة الإختصاص في مادة الجرائم المرتكبة عبر الأنترنت مرتبطة إرتباطا وثيقا بمسألة تطبيق قانون العقوبات الفرنسي من حيث المكان .

وفي هذا الصدد قررت المحكمة الإبتدائية في باريس باختصاص القاضي الجنائي الفرنسي بنظر جرائم الأنترنت ، إذا وصل موقع الأنترنت داخل الأراضي الفرنسية بغض النظر عن مكان السلوك الإجرامي.

كما جاء في إحدى قرارات الغرفة الجنائية لمحكمة النقض الفرنسية الصادر بتاريخ 9 سبتمبر 2008 في قضية متعلقة بإحدى المقالات الصادرة في الجريدة الفرنسية والذي أعيد نشره في جريدة إيطالية ، وتم بمقتضى القرار نقض الحكم الصادر من طرف قضاة الموضوع الذين تمسكوا باختصاصهم ، واعتبر (القرار) أنّ المقال المنشور في الجريدة الإيطالية لم يتم إصداره في فرنسا على النسخة الورقية وإنّما على شبكة الأنترنت من خلال موقع www.ifoglio.it والذي كان محررا باللغة الإيطالية ولم يكن موجها للجمهور في الإقليم الفرنسي ، وبالنتيجة لا جريمة ولا اختصاص للقاضي الجنائي الفرنسي [3] .

نفس الشيء بالنسبة للمشرع الأردني الذي أخذ بمبدأ إقليمية الجريمة بصفة عامة وإقليمية الجريمة الإلكترونية بصفة خاصة ، واكتفى أن يكون الأردن هو مكان ارتكاب الركن المادي للجريمة أو على الأقل جزء يسير من هذا الركن سواءا كان مكان ارتكاب الفعل أو مكان حصول النتيجة

---

[1] معتز سيد محمد أحمد عفيفي ، المرجع السابق ، ص.35 ، 36 .

[2] Article 113-2 de la LOI N92-683 du 22 juillet 1992 portant réforme des dispositions générales du code pénal Français , JORF du 23 juillet 1992 , N169 .

[3] David Chilstein , Législation sur la cybercriminalité en France , In : Revue internationale de droit comparé , Société de législation comparée , Vol.62 , France , 2010 , N2 , PP.597-598 .

، ومثال ذلك أن يحتال المتهم عبر الأنترنت على المجني عليه داخل الأردن ليستولي على أمواله في الخارج [1] .

المطلب الثاني : الإستثناءات الواردة على مبدأ إقليمية الجريمة الإلكترونية

بالرغم من أنّ مبدأ الإقليمية مازال يشكل أساس القانون الجنائي ، فإنّ ضرورة تحسين أداء هذا الأخير في مواجهة الجريمة أدّى إلى إيجاد قيود وإستثناءات على هذا المبدأ ، يستهدف الحد من الإرتباط المطلق للنصوص الجنائية بإقليم الدولة [2] ، فعلى سبيل المثال قد ترتكب الجريمة خارج إقليم الدولة ويكون أحد مرتكبيها أو المجني عليه من جنسية أخرى وهذا ما يعرف بمبدأ الشخصية ، أو قد تمس الجريمة إحدى المصالح الجوهرية للدولة وهو ما يعرف بمبدأ العينية ، وقد تقوم الدولة بمتابعة جريمة بغض النظر عن مكان ارتكاب الجريمة ، أو شخصية مرتكبيها ، أو شخصية المجني عليه وهو ما يطلق عليه بمبدأ العالمية . ونسعى من خلال هذا المطلب إسقاط هذه المبادئ على الجريمة الإلكترونية من خلال الفروع الآتية .

الفرع الأول : مبدأ شخصية الجريمة الإلكترونية

يقصد بهذا المبدأ ، أنّ قانون الدولة ينطبق على كل الأشخاص الذين ينتمون إليها أينما كانوا وأينما وجدوا ، دون الأشخاص الذين ينتمون إلى دولة أخرى حتى ولو كانوا هؤلاء الأشخاص يقيمون في ذات إقليم الدولة ، فلو قلنا أنّ القانون الجزائري شخصي التطبيق فهذا يعني ، أنّه يطبق على الجزائريين والجزائريات سواءا أكانوا متواجدين داخل التراب الوطني أو في بلد أجنبي ، فالعبرة بمبدأ شخصية القوانين هي بجنسية الشخص فطالما أنّه ينتمي إلى بلد ما تطبق عليه قوانين ذلك البلد بغض النظر عن مكان تواجده [3] ، ويقوم هذا المبدأ على أساس ما للدولة من سيادة على جميع رعاياها أينما وجدوا ، وذلك نظرا للرابطة التي تربط رعايا الدولة بدولتهم ، وهي علاقة لا تتقيد بمكان معين ؛ بل تتسع لتشمل جميع الأمكنة التي يوجد بها أحد من مواطنيها ، فهؤلاء المواطنون هم الذين وضعت التشريعات من أجلهم ، ومن ثم يجب أن يخضعوا لها حيثما وجدوا.

---

[1] رنا العطور ، البعد المكاني لقانون العقوبات الأردني دراسة مقارنة مع التشريع الفرنسي ، مجلة جامعة النجاح للأبحاث (العلوم الإنسانية) ، مجلد 25 ، نابلس ، فلسطين ، 2011 ، العدد 7 ، ص.1823 .

[2] صلاح هاشم ، التنمية والجريمة المعولمة ، سياسات الإفقار والهدم الخلاق ، الطبعة الأولى ، أطلس للنشر والإنتاج الإعلامي ، مصر ، 2017 ، ص.143

[3] حمزة خشاب تحت إشراف مولود ديدان ، المرجع السابق ، ص.116 .

ويعتبر حق الدولة في السيادة على مواطنيها نتيجة طبيعية بحكم أنّ المواطن يمثل عنصر الشعب في الدولة التي لا تقوم لها قائمة بغيره [1] .

وإذا كان الأصل هو تطبيق قانون العقوبات تطبيقا إقليميا طبقا لما تقتضي به الفقرة الأولى من المادة الثالثة منه ، إلاّ أنّ المصلحة العامة للدولة قد تقتضي الخروج على هذا الأصل ، ويسمح للدولة بمعاقبة مرتكبي بعض الجرائم المقترفة خارج الإقليم الجزائري ، وقد كرس ذلك قانون العقوبات عندما نص في مادته 3 فقرة 2 على ما يلي : " كما يطبق (قانون العقوبات) على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم الجزائية الجزائرية طبقا لأحكام قانون الإجراءات الجزائية " [2] .

ويؤدي هذا الإستثناء إلى تطبيق قانون العقوبات تطبيقا شخصيا أي سريان أحكامه على كل من يحمل جنسية الدولة التي ارتكب جريمته خارج إقليمها .

وممّا تجب الإشارة إليه هو أنّ هذا المبدأ يتخذ وجهان ؛ وجه إيجابي ويعني تطبيق القانون الجنائي على كل من يحمل جنسية الدولة ولو ارتكب الجريمة خارج إقليمها ، ووجه سلبي والمقصود به تطبيق القانون الجنائي على كل جريمة يكون فيها المجني عليه وطنيا والجاني أجنبي والجريمة وقعت خارج إقليم الدولة ، وبالرجوع إلى المشرع الجزائري نجد أنّه على غرار بعض التشريعات الأجنبية كالتشريع الفرنسي [3] والتشريع المصري [4] قد اعتدّ هو الآخر بهذا المبدأ حسب نص المادتين 582 و 583 من قانون الإجراءات الجزائية والمادة 591 فقرة 2 من ذات القانون التي أكدت على اختصاص الجهات القضائية الجزائرية بالنظر في الجنايات والجنح التي ترتكب على متن

---

[1] محمد سعيد جعفور ، مدخل إلى العلوم القانونية ، الجزء الأول الوجيز في نظرية القانون ، الطبعة التاسعة عشرة، دار هومه للطباعة النشر والتوزيع ، الجزائر ، 2012 ، ص.231 .

[2] المادة 3 فقرة 2 من الأمر رقم 66-156 المؤرخ في 8 جوان 1966 والمتضمن قانون العقوبات .

[3] أخذ بمبدأ الشخصية الإيجابي طبقا للمادة 113 فقرة 6 من قانون العقوبات ومبدأ الشخصية السلبي طبقا للمادة 113 فقرة 7 من نفس القانون .

[4] أخذ هو الآخر بمبدأ الشخصية الإيجابي من خلال المادة 219 من قانون رقم 150 لسنة 1950 والمتضمن قانون الإجراءات الجنائية والمادة 3 من قانون رقم 58 المؤرخ في 31 جويلية 1937 والمتضمن قانون العقوبات، جريدة رسمية مؤرخة في 5 أوت 1937 العدد رقم 71 ، وبمبدأ الشخصية السلبي من خلال المادة 3 فقرة 2 و5 من قانون رقم 175 المؤرخ في 14 أوت 2018 المتعلق بمكافحة جرائم تقنية المعلومات ، جريدة رسمية مؤرخة في 14 أوت 2018 ، العدد 32 مكرر (ج) .

طائرات أجنبية إذا كان الجاني أو المجني عليه جزائري الجنسية [1] ، دون أن ننسى أنّ المشرع قد أدخل على المادة 588 من ذات القانون تعديلا وتميما بمقتضى الأمر رقم 15-02 المؤرخ في 2015/07/23 والتي من خلالها أكد على اختصاص القانون الجزائري بالنظر في كل جريمة سواء كانت جناية أو جنحة مرتكبة في الخارج من قبل أجنبي وترتكب إضرارا بمواطن جزائري[2].

وعليه لنفترض أنّ مواطن جزائري أثناء تواجده في فرنسا قام بنصب واحتيال مواطن آخر عبر شبكة الأنترنت ، فحسب المادتين 582 و 583 السابقتين الذكر من قانون الإجراءات الجزائية ، فإنّه يمكن متابعة ومحاكمة هذا المواطن في الجزائر ، كما أنّ الجريمة وقعت خارج التراب الوطني من طرف جزائري ، ولكن بشرط عودة الجاني إلى الجزائر وثبوت عدم الحكم عليه نهائيا في الخارج أو أن يثبت في حالة الحكم بالإدانة أنّه قضى العقوبة أو سقطت عنه بالتقادم أو حصل على العفو عنها ، وهذا كله مع مراعاة الإتفاقيات الدولية ومبدأ المعاملة بالمثل في إطار المساعدة القضائية المتبادلة [3] ونفس الشيء بالنسبة للجريمة المعلوماتية المرتكبة في الخارج من قبل أجنبي ضد جزائري ، إذ تجوز متابعته ومحاكمته على هذا الفعل .

الفرع الثاني : مبدأ الإختصاص العيني للجريمة الإلكترونية

يقصد بالتطبيق العيني لقانون العقوبات سريان أحكامه على كل أجنبي يرتكب جريمة خارج التراب الوطني بصفته فاعل أصلي أو شريك في جناية أو جنحة ضد أمن الدولة الجزائرية أو مصالحها الأساسية أو المحلات الدبلوماسية والقنصلية الجزائرية أو أعوانها ، أو تزييفا لنقود أو أوراق مصرفية وطنية متداولة قانونا في الجزائر أو أي جناية أو جنحة ترتكب إضرارا بمواطن جزائري [4] ، والجدير بالذكر أنّ هذه المادة قبل تعديلها كانت أحكامها مقتصرة فقط على الجنايات والجنح الماسة بسلامة الدولة الجزائرية أو تزييف النقود أو الأوراق المصرفية مّما يبيّن أنّ المشرع

---

[1] المواد 582 ، 583 و591 فقرة 2 من الأمر رقم 66-155 المؤرخ في 8 جوان 1966 ، والمتضمن قانون الإجراءات الجزائية الجزائري .

[2] المادة 588 من الأمر رقم 66-155 المؤرخ في 8 جوان 1966 ، والمتضمن قانون الإجراءات الجزائية والمعدلة والمتممة بالأمر رقم 15-02 المؤرخ في 23 جويلية 2015 ، جريدة رسمية مؤرخة في 23 جويلية 2015 ، العدد 40 .

[3] المادتين 16و17 من قانون رقم 09-04 المؤرخ في 5 أوت 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها .

[4] المادة 588 من الأمر رقم 66-155 المؤرخ في 8 جوان 1966 ، والمتضمن قانون الإجراءات الجزائية والمعدلة والمتممة بالأمر رقم 15-02 .

الجزائري قد وسّع الحماية لتشمل أيضا المصالح الأساسية والمحلات الدبلوماسية والقنصلية الجزائرية أو أعوانها وكذا كل جناية أو جنحة ترتكب إضرارا بمواطن جزائري .

ففي هذه الحالة لسنا بصدد تطبيق مبدأ إقليمية قانون العقوبات، لأنّ المجرم لم يرتكب الجريمة داخل الإقليم الجزائري ، ولسنا بصدد تطبيق هذا القانون تطبيقا شخصيا لأنّ المجرم أجنبي ، بل نحن بصدد التطبيق العيني له ، الذي ينظر فيه إلى مساس الجريمة بكيان الدولة ومصالحها الأساسية.

وعلى هذا الأساس قد مدّ المشرع الجزائري اختصاص القاضي الجنائي الوطني لمعاقبة المجرمين الأجانب الذين يرتكبون جرائم معلوماتية خارج الإقليم الجزائري بحيث يمكن للعدالة الجزائرية مباشرة الدعوى الجزائية ضدهم .

وزيادة على قواعد الإختصاص المنصوص عليها في قانون الإجراءات الجزائية (المادة 588 المعدلة والسابقة الذكر والتي نحن بصدد دراستها) ، فإنّ المشرع منح الإختصاص للمحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني وهذا حسب المادة 15 من قانون 09-04 السابق الذكر .

هذا كله بالإضافة إلى المساعدة القضائية الدولية المتبادلة المنصوص عليها في المادة 16 من نفس القانون والتي من خلالها يمكن جمع الأدلة الخاصة بالجريمة الإلكترونية عن طريق الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته ، هذه الأخيرة يمكنها تبادل المعلومات مع مثيلاتها الأجنبية بغرض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي جرائم المعلوماتية والتعرف عليهم [1] ومن ثم تسهيل متابعتهم وجلبهم إلى المثول أمام المحاكم الجزائرية في إطار الإتفاقيات والمساعدة القضائية الدولية .

وبالرجوع إلى القانون المصري نجد أنّه هو الآخر قد أخذ بمبدأ العينية وهذا من خلال الفقرة 2 من المادة 2 من قانون العقوبات والتي نصت على أنّه تسري أحكام هذا القانون أيضا على كل من ارتكب في خارج القطر جريمة من الجرائم الآتية :

[29] المادة 9 من المرسوم الرئاسي رقم 19-172 المؤرخ في 6 جوان 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها وتنظيمها وكيفيات سيرها ، جريدة رسمية مؤرخة في 9 جوان 2019 ، العدد 37 .

(أ) جناية مخلة بأمن الحكومة ممّا نص عليه في البابين الأول والثاني من الكتاب الثاني من هذا القانون

(ب) جناية تزوير ممّا نص عليه في المادة 206 من هذا القانون .

(ج) جناية تقليد أو تزييف أو تزوير عملة ورقية أو معدنية ممّا نص عليه في المادة 202 أو جناية إدخال تلك العملة الورقية أو المعدنية المقلدة أو المزيفة أو المزورة إلى مصر أو إخراجها منها أو ترويجها أو حيازتها بقصد الترويج أو التعامل بها ممّا نص عليه في المادة 203 بشرط أن تكون العملة متداولة قانونا في مصر [1] .

وباستقراء هذه المادة يلاحظ أنّ الإختصاص العيني للجرائم يرتكز أساسا على الجنايات الماسة بأمن الحكومة وجنايات التزوير ، لذلك كان لزاما على المشرع توسيع هذا الإختصاص ليشمل مصالح جوهرية أخرى .

وعلى إثر ذلك تدخل المشرع المصري بسن قانون آخر والذي من خلاله وسع الإختصاص العيني للجرائم وهو القانون المتعلق بمكافحة جرائم تقنية المعلومات السابق الذكر ، حيث نص في فقرته الخامسة على سريان أحكام هذا القانون على كل أجنبي ارتكب خارج مصر جريمة من شأنها إلحاق ضرر بأي من مواطني مصر العربية أو المقيمين فيها أو بأمنها أو بأي من مصالحها ، في الداخل أو الخارج متى كان هذا الفعل معاقبا عليه في الدولة التي وقع فيها .

لذلك مثلا ، إذا قام أحد الأجانب خارج الإقليم المصري باختراق موقعا أو بريدا إلكترونيا أو نظاما معلوماتيا يدار بمعرفة أو لحساب الدولة المصرية بقصد الإعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية فإنّ أحكام هذا القانون تسري عليه ، وهذا كله مع مراعاة الإتفاقيات الدولية والإقليمية والثنائية المصادق عليها ، أو تطبيقا لمبدأ المعاملة بالمثل من أجل تبادل المعلومات التي من شأنها تسهيل عملية الكشف على مرتكب الجريمة وتحديد مكان وجوده[2].

الفرع الثالث : مبدأ عالمية الجريمة الإلكترونية وموقف المشرع الجزائري منه

[1] المادة 2 فقرة 2 من قانون رقم 58 لسنة 1937 المؤرخ في 31 جويلية 1937 المتضمن قانون العقوبات المصري .

[2] المادة 4 والمادة 20 من قانون رقم 175 لسنة 2018 والمتعلق بمكافحة جرائم تقنية المعلومات المصري .

نظرا لتطور القانون الجنائي ، أصبح من الضروري إيجاد مبدأ آخر لمواجهة الجرائم الدولية الماسة بمصالح وقيم المجتمع الدولي [1] ، فهو تأكيد دولة اختصاصها على الجرائم المرتكبة على إقليم دولة ما من طرف أشخاص تابعين لدولة أخرى ضد مواطنين حاملين جنسية دولة ثالثة ، بمعنى أنّ عالمية النص الجنائي تقتضي مطالبة الدولة الحق في المتابعة في جميع الظروف وعلى خلاف المبادئ التقليدية المتعلقة بالإقليمية ، الجنسية والعينية أي بصرف النظر عن مكان ارتكاب الجريمة ، أو شخصية مرتكبيها ، أو شخصية المجني عليه ، وبغض النظر عمّا إذا كان معاقبا عليها في الدولة التي ارتكب فيها [2] .

وبالرجوع إلى المشرع الجزائري نجد أنّه لم ينص على هذا المبدأ وهو نفس موقف المشرع المصري ، على عكس المشرع الفرنسي الذي أخذ بهذا المبدأ في الفقرة 12 من المادة 113 من قانون العقوبات والتي نص بموجبها على أن : " يطبق قانون العقوبات الفرنسي على الجرائم المرتكبة ما وراء البحر الإقليمي ، طالما أنّ الإتفاقيات الدولية والقانون ينص على ذلك " .

وباستقراء المرسوم رقم 2006-581 والمتعلق بإصدار المعاهدة الدولية الخاصة بالجريمة الإلكترونية والمعتمدة في بودابست[3] نلاحظ أنّ المادة 22 منه والخاصة بمسألة الإختصاص قد تحفظ المشرع الفرنسي بشأنها ، حيث اعتبر أنّه يملك الحق في عدم الإختصاص عندما لا تدخل الجريمة الإلكترونية في الإختصاص الإقليمي لأي دولة .

لذلك يتضح جليا أنّ موضوع عالمية الجريمة الإلكترونية من المواضيع الشائكة التي تتطلب إبرام معاهدات دولية في هذا الصدد ، وهو أمر صعب ومحدود جدا لأنّه يصطدم غالبا بمبدأ سيادة الدول والأمن الوطني لها [4] .

---

[1] معتز سيد محمد أحمد عفيفي ، المرجع السابق ، ص.43 .

[2] بديار ماهر وآخرون ، الإختصاص العالمي لمحاكم الجنايات الوطنية ، مجلة جامعة تكريت للعلوم القانونية والسياسية ، المجلد 5 ، العراق ، 2013 ، العدد17 ، ص.119 .

[3] Article 22 du décret N2006-580 du 23 mai 2006 portant publication de la convention sur la cybercriminalité , faite à Budapest le 23 novembre 2001, JORF du 24 mai 2006 , N120 .

[4] La coopération internationale et bilatérale en matière de cybersécurité : enjeux et rivalités , Laboratoire de l'IRSEM (Institut de Recherche Stratégique de l'Ecole Militaire) , Ministère De La Défense et Des Anciens Combattants , Paris , France , 2013 , N16 .

خاتمة :

في الختام يمكن القول بأنّ الجريمة المعلوماتية هي جريمة عالمية لا تعرف حدودا معينة فهي في نمو وتطور سريع ّمما ينجم عنه صعوبة ملاحقة مرتكبيها وكذا ضبطهم ، إضافة إلى مسألة الإختصاص القانوني والقضائي والإشكالية المترتبة عنها والتي حاولنا تسليط الضوء عليها في هذا المقال ؛ وعلى هذا الأساس اعتمد المشرع الجزائري على مبدأ إقليمية الجريمة الإلكترونية كأصل عام وأخذ بالإستثناءات الواردة عليه على غرار مبدأ الشخصية ومبدأ العينية ، كما أصدر في هذا الشأن قانونا في مجال مكافحة هذه الجريمة وهو القانون رقم 09-04 المؤرخ في 2009/08/05 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، وأنشأ بمقتضاه هيئة وطنية للوقاية من هذه الجرائم والتي خولها مهمة تبادل المعلومات مع نظيراتها في الخارج من أجل الكشف عن المجرمين ومتابعتهم وتوقيع العقوبة عليهم في إطار الاتفاقيات الدولية والمساعدة القضائية الدولية ، وهذا كله لتقليص إشكالية الاختصاص المتولدة عن هذه الجريمة.

إضافة إلى ذلك فإنّ المشرع الجزائري لم يأخذ بمبدأ عالمية الجريمة ، لذلك كان من الأجدر الاعتداد به خصوصا في هذا النوع من الجرائم كونها تهدد سلامة وأمن المجتمع الدولي والتنمية الاقتصادية .

المتابعة في الجريمة المعلوماتية و عوائق الإثبات

Follow-up mechanisms in cyber crime and evidence of impediment

د. بن عودة صليحة

معهد الحقوق و العلوم السياسية

أستاذة محاضرة قسم ب

المركز الجامعي مغنية - الجزائر

مقدمة

ساهمت الثورة المعلوماتية التي يشهدها العالم في عصرنا هذا في تطوير معاملات الأفراد وتسهيلها وذلك في شتى مجالات الحياة المختلفة خاصة بظهور الانترنت والتي وضعت العالم كله في قرية صغيرة نظرا لما تمتاز به من سرعة في تبادل المعلومات والبيانات ما أدى إلى تكثيف المعاملات بواسطتها بين الأفراد.

إلا أن هاته المعاملات أدت إلى ظهور مشاكل في مجالات القانون المختلفة وخاصة القانون الجنائي، وذلك نظرا للجرائم التي أصبحت تعترضها والتي تجسدت في ظاهرة الجريمة المعلوماتية[1].

وإن كانت التشريعات العقابية التقليدية قد تناولت الجرائم التقليدية التي تقع على الأموال والأشخاص وغيرها من التجريم، فإن هذه القوانين قد لا تطال غالبية الجرائم التقنية المعلوماتية، وذلك باختلاف هذه الأخيرة عن سابقتها في الطبيعة أو في المكان أو في المحل.

وفي الواقع فإن القانون الجزائي لا يتطور دائما بنفس السرعة التي تتطور بها التكنولوجيا أو مهارة الذهن البشري في تسخير المبتكرات للاستخدام السيء. فالأشكال المستجدة للجريمة لم يقتصر اعتداؤها على القيم المادية التي كانت محمية بقانون العقوبات، بل امتد هذا الاعتداء إلى القيم المعنوية مثل المعلومات والمعطيات وغير ذلك، فأصبحت النصوص التقليدية في قانون العقوبات عاجزة عن مواكبة هذه الأشكال المستحدثة من الإجرام المعلوماتي.

بالإضافة إلى أن جرائم الحاسب الآلي ليس لها آثار خارجية، وإنما تنصب على البيانات والمعلومات والمستندات المخزنة في نظم المعلومات والبرامج وبالتالي عدم الحصول على آثار مادية تشكل دليلا لإثبات الجريمة المعلوماتية الواقعة في غياب أعمال العنف والاقتحام والتكسير على

---

[1] - طعباش أمين، الحماية الجنائية للمعاملات الالكترونية، الطبعة الأولى، مكتبة الوفاء القانونية، الاسكندرية، 2015، ص14

خلاف الجرائم العادية يصعب إثبات الجريمة، كما أن ارتكابها يقع في الخفاء وتعمد الجاني عدم ترك أي دليل إدانة بعد ارتكابه للجريمة[1].

و تكمن أهمية البحث في مدى الخطورة التي تُشكلها الجرائم المعلوماتية إذ إنها تطال الحق في الحصول على المعلومات وتمس حرمة الحياة الخاصة للأفراد وتُهدد الأمن الوطني وتُؤدي إلى فقدان الثقة بالتقنية وغيرها من مفاصل الحياة العامة المختلفة.

بينما تهدف الدراسة إلى معرفة أهمية الاستدلالات وضوابط إثبات الجريمة المعلوماتية، وكذلك التعرف على كيفية إثباتها بالشهادة والإقرار والخبرة الفنية، بالإضافة إلى معرفة معوقات المتابعة والإثبات.

سنتناول في هذا البحث دراسة الجرائم المعلوماتية في نطاق إجراءات المتابعة من أجل إبراز إثبات الجريمة محاولين قدر الإمكان وضع اليد على بعض الحلول الناجعة لمكافحة هذه الظاهرة الإجرامية، مستندين في ذلك إلى عرض وتحليل النصوص القانونية المتعلقة بهذا المجال.

وتتمثل مشكلة البحث في مدى الصعوبة التي تُواجهها إجراءات التحقيق في هذا النوع من الجرائم والمتمثلة في إخفاء الجريمة وسهولة وسرعة محو أو تدمير أدلة ومعالم الجريمة والضخامة البالغة لكمية البيانات المراد فحصها على الشبكة، وتبرز كذلك صعوبات في مسائل جمع الأدلة من المعاينة والتفتيش والضبط وغيرها من الإجراءات، فضلاً عن الطابع العالمي الذي تمتاز به هذه الجرائم لكونها من الجرائم التي تتجاوز عنصري الزمان والمكان. ومنه نطرح الإشكالية التالية: **ماهي الصعوبات والمعوقات التي تواجه جهات البحث والتحري في الكشف عن الجريمة المعلوماتية؟**

للإجابة على هذه الإشكالية سيتم تقسيم هذا الموضوع إلى قسمين يتضمن القسم الأول المعوقات المتعلقة بالجريمة في حد ذاتها، أما المعوقات المتعلقة بإثباتها سيتم التطرق إليه من خلال القسم الثاني.

المبحث الأول: المعوقات المتعلقة بالجريمة في حد ذاتها

إن موضوع أو محل الجريمة الالكترونية يعتبر أهم خاصية تميز بها هذه الأخيرة عن غيرها من الجرائم التقليدية، حيث تكون المعلومات والبرامج هي محل الاعتداء وهي عبارة عن نبضات الكترونية، وعليه نكون أمام ظاهرة إجرامية مستحدثة ذات طبيعة خاصة فالجريمة الالكترونية إفراز ونتاج تقنية المعلومات واتساع نطاق تطبيقها في المجتمع، مما أعطى لونا وطابعا قانونيا خاصا

---

[1]- عبد الفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الطبعة 1، 2006، ص142-143.

وميزها بمجموعة من الخصائص مختلفة عن الجرائم التقليدية لصعوبة تحديدها **(المطلب الأول)**، وهذه الخصائص منها ما يتعلق بالشخص الذي يقدم على ارتكاب هذه الجريمة فميزته عن المجرم التقليدي (**المطلب الثاني**).

المطلب الأول: صعوبة تحديد الجريمة المعلوماتية:

إن التطرق إلي مفهوم الجريمة المعلوماتية تكتنفه صعوبة خاصة، وذلك يرجع إلي أن هذا النمط من الإجرام يعتبر من الأنماط المستحدثة، التي رافقت التطور التكنولوجي هذا من جهة، ومن جهة أخري فإنها تتسم بتنوعها وتعدد تسمياتها، لهذا يصعب تحديد أركان هذه الأخيرة (الفرع الأول)، ومن حيث وصفها لارتباط هذا النوع من الجرائم بأكثر من إقليم دولة واحدة، وهنا تظهر أهمية وفائدة التعاون الدولي (الفرع الثاني).

الفرع الأول: من حيث أركان الجريمة

يرجع السبب الرئيسي في عدم القدرة على تحديدها إلى صعوبة اكتشاف أركانها، فإضافة إلى الشرط المبدئي في كل جريمة ونقصد به الركن الشرعي، لابد من إثبات ركن مادي ملموس يعبر عن إرادة المجرم المعلوماتي.

أولا/ الركن الشرعي:

هناك العديد من الجرائم الالكترونية والتي لا ينطبق عليها أي وصف قانوني، فكان لزاما على أي مشرع أن يأخذ هذا التقدم التكنولوجي بعين الاعتبار، وأن يقوم بتطوير الوسائل اللازمة، أهمها قواعد التجريم لردع هذا الإجرام المعلوماتي. والذي أخذ بالتزايد والانتشار بشكل مذهل دون معوقات قانونية سواء من المشرع أو المجتمع ككل عن طريق توعية الأفراد بالأضرار التي تخلفها هذه السلوكيات. وفي العديد من الدول تبقى الجهود على المستوى الفردي فقط من قبل أصحاب الأجهزة والمؤسسات المالية والاقتصادية والتي تستخدم أجهزة الحاسوب فتضع بعض أنواع الحماية والشفرات الالكترونية لردع من يخترق برامجها ويحاول الاعتداء على معلوماتها وأجهزتها. فكيف تكون محاربة هذا النوع من الإجرام إذ أن العديد من القضايا التي عرضت على القضاء الفرنسي تضاربت فيها الأحكام وحدث الخلاف فيما إذا كانت هذه الأفعال يصدق عليها وصف السرقة وفقا للمادة 379 من قانون العقوبات الفرنسي، بالمفهوم التقليدي أم أن الفعل يحتاج إلى نص خاص.

فقد كانت الاتجاهات متضاربة فيما يتعلق بتصوير المستندات بالمفهوم التقليدي عن طريق وسائل التصوير المخصصة لذلك، أما الآن فإن جهاز الكمبيوتر نفسه باستطاعته أن يقوم بنسخ

المعلومات الموجودة في أي جهاز دون أن يتلفها. فهل يعد هذا من قبيل السرقة والتصوير التقليدي؟ وإذا قام المجرم المعلوماتي بالإطلاع فقط على المعلومات بالنظر، فهل يمكن أن يحاسب على هذا الفعل وتحت أي تكييف؟ وهناك إشكالية أخرى تتعلق بالمصطلحات المستخدمة والغريبة عن لغة القانون الجنائي مثل القرصنة والتي اعتدنا عليها في المجال البحري، فالعديد من الكتاب عبروا عن فعل السرقة عبر الإنترنت بالقرصنة، وأطلق هذا المصطلح على عملية نسخ البرامج، ولاشك أنه يعكس مدى خطورة وبشاعة الفعل المرتكب[1].

ثانيا/ الركن المادي:

يجب أن يكون الفعل أو السلوك المجرم الذي يقوم به الجاني ملامسا لأرض الواقع حتى يمكن التحقق منه وإثباته، ونحن لا نتكلم عن الركن المادي في الجرائم المعلوماتية التي تكون وسيلة ارتكابها معلوماتية، حيث لا يمكن حصرها تحت تكييف واحد، فقد تشكل واقعة قذف أو سب أو تهديد أو تحريض على أفعال غير مشروعة بشكل مطابق للجريمة التقليدية المقررة في قانون العقوبات ويمكن أن ينطبق التفسير الوارد في النصوص التقليدية على هذه الصور.

بينما الذي يثير صعوبة هو الجرائم التي يكون موضوعها المال المعلوماتي المعنوي، مثل إساءة استخدام البريد الالكتروني عن طريق الرسائل المفخخة وتعطيل الشبكات عن طريق الفيروسات، التي قد تدمر كليا أو جزئيا المعلومات المخزنة أو النظام المعلوماتي أو التلاعب ببطاقات الائتمان عبر شبكة الإنترنت[2]. فهذه الجريمة تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والإنترنت، مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة، وذلك لسهولة محو الدليل من قبل الفاعل[3] عن طريق التلاعب ير المرئي في النبضات الالكترونية التي يتم تسجيل البيانات عن طريقها، كما أن الوصول إلى المجرم في الوقت الذي يبدأ بالاتصال وارتكابه للجريمة ليس بالأمر السهل لأن الاتصال يمر على العديد من الحواسيب ومن خلال التقنية يمكن الحصول على عناوين الحواسيب المتصلة مباشرة

---

[1]- غنية باطلي، الجريمة الالكترونية (دراسة مقارنة)، الدار الجزائرية للنشر والتوزيع، الجزائر، 2016، ص44-45

[2]-غنية باطلي، مرجع سابق، ص45

[3]- نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008، ص56.

بها، ولكن إن تم معرفة المصدر الأصلي فقد يكون العنوان خاطئ.ومما يزيد في صعوبة إثباتها هو عدم مساعدة المجني عليهم السلطات فيما لو تم اكتشافها[1].

وأكثر من ذلك فإن أغلب القواعد الجنائية غير كافية لوجود صعوبات أخرى تتمثل في البحث عن الدليل وجمعه ومشكلة قبوله إن وجد ومدى مصداقيته وحجيته في إثبات وقائع الجريمة. وعليه فيجب الإسراع في إيجاد منظومة قانونية واستحداث نصوص جديدة تتلاءم والمستحدثات التي فرضتها هذه التكنولوجيا[2].

في الأخير نقدم بعض الأسباب التي قام بجمعها محمد محمد شتا[3] والتي تعد مظاهر لصعوبة الجريمة المعلوماتية وهي خمس:

- أنها جريمة لا تترك أثرا ماديا ملموسا.
- أنها جريمة يصعب فنيا الاحتفاظ بآثارها إن وجدت.
- أنها جريمة يصعب على المحقق التقليدي أن يفهم حدودها الإجرامية وما تخلفه من آثار غير مرئية.
- أنها جريمة تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها
- أنها جريمة بيضاء تعتمد على قمة الذكاء في ارتكابها.

ثالثا/ الركن المعنوي:

لقد أثر استخدام الوسائل التقنية الحديثة في ارتكاب الجريمة على الفكرة أو التصور القديم المتعارف عليه بشأن الانحطاط الثقافي والفكري للمجرم والظروف الاجتماعية القاسية لهذا الشخص المبرز لخطورته الإجرامية على نحو ملفت للانتباه يستدعي الخوف وأخذ الحيطة والحذر منه. فالوضع اليوم مختلف حيث أصبح المجرم المعلوماتي يتمتع بقدر من الفطنة والذكاء ونصيب وافر من التعليم والاختصاص، فبالنسبة للجرائم المعلوماتية لابد من توافر قدر كبير من المعرفة

[1]- محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية، 2001، ص46

[2] -Mohamed BOZABAR, La criminalité informatique sur l'internet, Journal Of Law Academic, N :01, volume 26, Faculté de droit, université du Koweit, 2002, p73

[3]- محمد محمد شتا، نفس المرجع، ص103.

في مجال تقنية المعلومات والحاسوب حيث أصبحت أصابع الاتهام موجهة للمتعلمين وذوي الاختصاص[1].

ومن المتصور غالبا أن لا تقع الجريمة المعلوماتية إلا بصورة عمدية سبقها التفكير في الحصول على المعلومة أو اختراق الشبكة. والأصل في الجرائم هو العمدية إلا ما استثني بنص، وهناك من الجرائم ما يتطلب المشرع إرادة ارتكاب السلوك وتحقق النتيجة، حيث يكتفي بتوافر القصد الجنائي العام بصورتيه العلم والإرادة كالدخول إلى أنظمة المعلومات وتدمير المعلومات الموجودة بها أو تدمير ذاكرة الحاسب بعد نسخ ونقل المعلومات التي كانت عليها من أجل طمس الدليل. لكن قد يتطلب المشرع إضافة إلى القصد الجنائي العام قصدا جنائيا خاصا كضرورة توافر نية التملك للأموال المتحصل عليها من سرقة بطاقات الائتمان وتحويلها إلى حسابه الخاص.

إلا أن هذا لا يعني أن هذه الجريمة لا تحقق بطريقة غير عمدية عن طريق الخطأ أو الصدفة، كتدمير أجهزة المؤسسة نتيجة إفراط الموظف المسؤول الذي استخدم الجهاز العائد لها في عمليات لحسابه الخاص معتمدا على قدرته ومهارته، أو استخدام القرص المرن الخاص به في أجهزة المؤسسة ونقل الفيروسات لها والدخول له ميزة غير مادية فقد يعلم الشخص أنه دخل بمحض الصدفة أو عن طريق الخطأ إلا أن هذه الجرائم هي جرائم امتناع يصعب تقديم الدليل لإثباتها، فقد يزعم الجاني أنه كان على وشك الانفصال أو يدعي بأنه يتجول في جزء ضيق من النظام. وعمليا لا يمكن التحقق من هذا الإدعاء. كذلك تثير حالة تجاوز مجال التصريح مشكلة الإثبات حيث أن إثبات القصد الجنائي للفاعل الذي يتمتع بتصريح محدد صعب، إضافة إلى أن أنظمة الحاسبات مفتوحة على بعضها[2].

الفرع الثاني: من حيث وصف الجريمة

إن عدم القدرة على إلقاء القبض على الفاعل يعتبر من الأسباب التي تؤدي إلى صعوبة إثباتها، وهذا راجع إلى الطابع الدولي لهذه الشبكة وما يثيره هذا الأمر من مشاكل وصعوبات جمة. وحتى وإن وجد الفاعل فيكون يكون من الصعب تنفيذ العقاب عليه. إضافة إلى أن الأضرار المترتبة على هذا النوع من الجرائم تكون فادحة وجسيمة.

---

[1]- فايز الظفيري، الأحكام العامة للجريمة الالكترونية، مجلة العلوم القانونية والاقتصادية، العدد الثاني، كلية الحقوق، جامعة عين شمس، 2002، ص520.

[2]- JEAN FRANCOIS CASILE, le code pénal à l'épreuve de la délinquance informatique, presse universitaires D'AIX, marseille, PUAM, 2002, p97.

أولا: الجريمة المعلوماتية جريمة عابرة للحدود:

يعتبر العالم هو مسرح الجريمة المعلوماتية كونها تقع على شبة الإنترنت العالمية، أي أنها لا تقع بمكان محدد كباقي الجرائم الجنائية. حيث تكون المسافة بين الجاني والمجني عليه آلاف الأميال، وقد تكون أمتارا معدودة، لأنه لا يجد حائل يقف أمام نقل المعلومات بين الحاسبات الآلية المتواجدة في مختلف دول العالم عبر شبكات الاتصال. حيث نجد أن مستخدم الإنترنت من دولة ومورد أو مقدم خدمة الاشتراك من دولة أخرى وشركة تكنولوجيا معالجة البيانات وإدخالها وتحميلها عبر الشبكة من دولة ثالثة[1].

فيمكن أن تقع الجريمة من الفاعل في دولة على مدني عليه في دولة أخرى في وقت يسير جدا مخلفة أفدح الخسائر خاصة في مجال التجارة الالكترونية وازدياد اعتماد البنوك عليها[2] .

إن الطابع الدولي لهذه الجريمة يثير العديد من الإشكالات والصعوبات لاسيما مشكلة تحديد المحكمة المختصة دوليا بالمنازعات الناشئة، القانون الواجب التطبيق، أدلة الإثبات وقبولها أمام قضاء دولة أخرى، ولهذا فمكافحة هذا النوع من الجرائم يتطلب تعاونا كبيرا بين تشريعاتها[3].

ثانيا: صعوبة تنفيذ العقاب على مرتكبها:

تتسم الجريمة المعلوماتية بعدم القدرة على منع حدوثها، إذ أن هذا المنع يتطلب وقوع الضرر ووجود متضرر يبلغ الجهات المعنية بالضرر الواقع عليه[4]، وحتى وإن تم التوصل إلى الجاني فيكون من الصعب توقيع العقاب عليه لوجود عدة معوقات يمكن إرجاعها إلى قلة التشريعات التي تواجه هذا النوع من الجرائم.

حيث نجد أفعال غير مشروعة التي لا تنطبق عليها أي وصف أو نص من قانون العقوبات خصوصا مع القيود التي ترد على القاضي الجنائي، حيث لا عقوبة ولا جريمة إلا بنص ومبدأ حضر القياس في مجال الجرائم وكذا مبدأ التفسير الضيق للنصوص.

---

[1]- محمد الصدفي، الضبط في الجريمة الإلكترونية، العدد 23، وكالة الأهرام للتوزيع، 2004، ص09.

[2] - M.QUEMENER et J.FERRY , cybercriminalité, defé mondial, 2éme édition, Economica, Paris, 2009,p 67.

[3]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الاسكندرية، 2007، ص 78

[4]- محمد الصدفي، مرجع سابق، ص9

إضافة إلى ذلك قلة الخبرة الفنية في التعامل مع الكمبيوتر لدى المشرع والقاضي وبالتالي يظهر ذلك في التأثير على تطبيق العقوبات على هؤلاء الجناة. ويمكن القول بأن الصعوبة ترجع كذلك إلى كل من الجاني والمجني عليه وطبيعة الجريمة في حد ذاتها[1].

ثالثا: الجريمة المعلوماتية جريمة فادحة الأضرار

إن الإقبال المتزايد على الحاسب الآلي والإنترنت في إدارة مختلف الأعمال في شتى المجالات زاد من حدة الأضرار والخسائر التي تخلقها هذه الجرائم، خصوصا بالنسبة للمؤسسات المالية والبنوك ومختلف الشركات التي تعتمد في خطة عملها على جهاز الحاسوب، وهناك عدة دراسات تشير بأن الأضرار الناجمة عن الجرائم المعلوماتية تفوق الأضرار الناتجة عن الإجرام التقليدي[2].

المطلب الثاني: صعوبة اكتشاف الجريمة المعلوماتية

تميز الجريمة المعلوماتية بصعوبة اكتشافها، وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة، حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم قليلة إذا قورنت بما يتم اكتشافه من الجرائم التقليدية، ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة المعلوماتية إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية، وكذلك اختفاء السلوك المكون لها، كما أن الجاني(**الفرع الأول**) يمكنه ارتكاب هذه الجريمة في دول وقارات أخرى، إذ أن الجريمة المعلوماتية جريمة دولية، وكذلك فإن قدرة الجاني على تدمير الإدانة في أقل من الثانية الواحدة يشكل عاملا إضافيا في صعوبة اكتشاف هذا النوع من الجرائم[3]، كما أن المجني عليه (**الفرع الثاني**) يلعب دورا رئيسيا في صعوبة اكتشاف وقوع الجريمة المعلوماتية[4].

الفرع الأول: صعوبات تعود للجاني

المجرم الذي يقترف الجريمة المعلوماتية، والذي يطلق عليه المجرم المعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية، فإذا كانت الجرائم التقليدية لا أثر فيها للمستويين

1- غنية باطلي، مرجع سابق، ص51.

2- محمد خليفة، المرجع السابق، ص38.

3-- الصغير ناصر محمد، مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس اتعاون لدول الخليج العربية ، مركز الإمارات للدراسات والبحوث الاستراتيجية، ابوظبي، 2008، ص12.

4- رستم، هشام محمد فريد، الجوانب الإجرامية للجوانب المعلوماتية، مجلة الأمن والقانون، العدد الثاني، شرطة دبي، 1993، ص16.

العلمي والمعرفي للمجرم في عملية ارتكابها باعتبارها قاعدة عامة[1]، فإن الأمر يختلف بالنسبة للجرائم المعلوماتية، فهي جرائم فنية تقنية في الغالب الأعم، ومن يرتكبها عادة يكون من ذوي الاختصاص في مجال تقنية المعلومات أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الانترنت، فعلى سبيل المثال، فإن الجرائم المعلوماتية ذات الطابع الاقتصادي مثل التحويل الالكتروني غير المشروع للأموال يتطلب مهارة وقدرة فنية تقنية عالية جدا من قبل مرتكبها، كذلك فإن البواعث على ارتكاب المجرم المعلوماتي لهذا النوع من الإجرام المعلوماتي قد تكون مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي[2].

كما أن هناك خصائص أخرى تميز المجرم المعلوماتي عن غيره من مرتكبي الجرائم والمتمثلة في:

- أنه إنسان اجتماعي، فهو لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به، بل إنه إنسان متوافق معه، وتزداد خطورته الإجرامية إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه

- أنه إنسان محترف وذكي، حيث يقوم بالتلاعب في بيانات وبرامج الحاسب الآلي لكي يمحو هذه البيانات أو يعطل استخدام البرامج عن طريق زرع الفيروسات أو استخدام القنابل المنطقية أو الزمنية ليشل حركة النظام المعلوماتي ويجعله غير قادر على القيام بوظائفه الطبيعية.

1- هواة ارتكاب الجرائم المعلوماتية: ويطلق عليهم مصطلح الهاكرز (Hacker's)، ويعني المتطفل، وهو ذلك الشخص الذي يدخل على شبكات وحاسبات الآخرين دون حق. يتميزون بقدر عال من الكفاءة التقنية، ويتفاخرون بقدرتهم على اختراق شبكات الحاسب الآلي بجهدهم الذاتي دون الاستعانة بأي تعليمات من أي مصادر، وأغلبهم صغار السن، مراهقون وشباب عاطل عن العمل. ويهدف هاوي ارتكاب الجرائم المعلوماتية إلى الحصول على المعلومات بشتى الوسائل، ويسخر قدراته في هذا المجال.

محترفو ارتكاب الجرائم المعلوماتية: ويطلق على هذه الفئة مصطلح Cracker's حيث يتميزون بالتخصص العالي في مجال الحاسب الآلي، وتعد هذه الطائفة من أخطر مجرمي المعلوماتية، حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم أو للجهات التي كلفتهم وسخرتهم لارتكاب جرائم الحاسوب، أو إلى تحقيق أغراض سياسية، وتتراوح أعمارهم مابين 25 و40 سنة،

المتطرفون من ذوي المثل العليا: تتألف هذه المجموعة من أشخاص يدافعون عن قضية أو غاية ليس لها علاقة بمصالحهم الشخصية المباشرة وهم على استعداد للانخراط في أنشطة إجرامية، وقد يكون وراء ذلك أسباب سياسية أو دينية أو تتعلق بحقوق الإنسان.

2- المويشير، تركي بن عبد الرحمن، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فعاليته، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009، ص25.

كما يتصف المجرم المعلوماتي بأنه على درجة عالية من الخبرة والمهارة في استخدام التقنية المعلوماتية، حيث يقوم بالدخول إلى أنظمة الحاسب الآلي وسرقة الأموال وارتكاب جرائم النصب والتجسس وزرع الفيروسات وغيرها من الجرائم التي تتطلب مستوى مهارة وخبرة كبيرة في ارتكابها.

كل هذه الصفات ساعدت هؤلاء المجرمين على ارتكاب جرائمهم، دون ترك أي أثر مادي يمكن من خلاله الكشف عن جرائمهم ومساءلتهم جنائيا[1].

الفرع الثاني: صعوبات تعود للمجني عليه

يمكن أن يكون ضحية هذه الجرائم أشخاص طبيعية أو معنوية طالما كانت تستخدم الحاسب الآلي في ممارسة أنشطتها الاقتصادية أو الاجتماعية أو حتى السياسية والعسكرية........الخ . وإن كان من الصعب تحديد نطاق هؤلاء الضحايا على وجه الدقة وذلك راجع أن هؤلاء لا يعلمون شيئا عنها إلا بعد أن تقع بالفعل.

وفي هذه الحالة يرى أنه من الحكمة عدم الإبلاغ عنها وغالبا ما يكون المجني عليه مؤسسة مالية أو مصرفا أو شركة ضخمة[2]، حيث تخشى مجالس إدارتها من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها إلى تضاؤل الثقة فيها من جانب المتعاملين معها، ويحبذ المحافظة على هذه الثقة أكثر من الكشف عن الجريمة. ولا يحبذون أن يكشفوا بأن نظامهم المعلوماتي قد تم اختراقه أو وقع ضده انتهاك.

وتتمثل هذه الصعوبات فيما يلي:

1) عدم إدراك خطورة الجرائم المعلوماتية من قبل المسئولين بالمؤسسات، وهذا يرجع إلى إغفال جانب التوعية لإرشاد المستخدمين إلى خطورتها، وبالنظر إلى بعض المؤسسات نجد أنها أسست نظم معلوماتها على تطبيقات خاصة من التقنية على أساس أنها تقدم لعملائها خدمات أسرع بدون عوائق ويكون ذلك على الجانب الأمني.

2) الحفاظ على سمعة بعض المؤسسات والأفراد، حيث يكون الإحجام عن الإبلاغ عن هذا النوع من الجرائم بسبب عدم رغبة الجهات المتضررة في الظهور بمظهر مشين أمام الآخرين، لأن

1- بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية، الجزائر، 2017، ص 41-42، وطعباش أمين، مرجع سابق، ص 22-23

2- حسنين طاهر داوود، جرائم نظم المعلومات، الطبعة الأولى، دار الحامد للنشر والتوزيع، الأردن، 2014، ص25.

تلك الجرائم ارتكبت ضدها، مما قد يترك انطباعاً بإهمالها أو قلة خبرتها أو عدم وعيها الأمني، ولم تتخذ الاحتياطات اللازمة لحماية معلوماتها.

3) تعد التقنية المستخدمة في نظم المعلومات مجال استثمار، ولذا تتسابق الشركات في تبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة وملحقاتها، وزيادة المنتجات واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الأمني، على سبيل المثال مستخدمو شبكة الانترنت عبر مزودي الخدمة وبطاقات الانترنت المدفوعة ليسوا مطالبين بتحديد هويتهم عند الاشتراك في خدمة الانترنت، أي أن مزود الخدمة لا يعرف هوية مستخدم الخدمة[1].

4) خشية بعض الجهات المتضررة من الحرمان من الخدمة، إذ أن الإفصاح عن التعرض لجريمة معلوماتية من شأنه حرمان شخص من خدمات معينة تتعلق بالنظام المعلوماتي، فقد يحرم الموظف في الجهة من خدمات معينة على الانترنت أو قد يحرم من خدمات الانترنت عموماً، حيث يتعرض لجريمة معلوماتية ناتجة عن الاختراق أو زيارته لأماكن غير مأمونة أو غير مسموح بزيارتها، وقد يكون سبب عدم الإبلاغ عن الجريمة عدم معرفة الضحية بوجود جريمة أصلاً، وعدم القناعة أنها يمكن أن تحدث في مؤسسته[2].

المبحث الثاني: المعوقات المتعلقة بالقواعد الإجرائية لمتابعة الجريمة المعلوماتية

إن اكتشاف الجريمة المعلوماتية أمر ليس بالسهل ولكن حتى في حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به كذلك الكثير من الصعاب، فالجريمة المعلوماتية تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والإنترنت، مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات الكترونية غير مرئية تنساب عبر النظام المعلوماتي مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمر في غاية السهولة[3].

1- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبع الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2011، ص223.

2- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، 2010، ص67-68.

3- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، 2008، ص 56.

المطلب الأول: صعوبات التحقيق في الجريمة المعلوماتية

يتميز التحقيق في الجرائم المعلوماتية بالعديد من المعوقات والصعوبات فنظرا لوقوع الجريمة المعلوماتية ضمن بيئة رقمية كامنة في أجهزة الحاسب الآلي والخوادم (serveur) والمضيفات والشبكات بمختلف أنواعها، أدت إلى ظهور نوع من التحدي للأجهزة المختصة بالبحث والتحري في تطبيق القواعد الإجرائية، والتي تنعكس على المجرم نفسه حيث يشعر أن الجهات الأمنية غير قادرة على اكتشاف أمره وأن خبرة القائمين على مكافحة الجريمة والتحقيق فيها لا تجاري خبرته، الأمر الذي يعطيه ثقة أكبر في ارتكاب المزيد من هذه الجرائم[1].

الفرع الأول: أهمية التحقيق في إثبات الجريمة المعلوماتية

إن إثبات أي قضية جنائية أو مالية أو أي من القضايا تعتمد على الإجراءات الأولية وطرق التحقيقات المتخذة من جهات الضبط، وعلى ضوء هذه الإجراءات وبإتباع الأساليب المناسبة يمكن التوصل إلى اكتشاف ملابسات أي جريمة مما يسهل على الجهات القضائية إثبات الجريمة ومن ثم إدانة المتهم.

وتتطلب طبيعة الجريمة المعلوماتية أساليب غير تقليدية في التحقيق لاكتشاف الدليل الرقمي ودعمه من قبل الفنيين المختصين، وذلك يستدعي اتخاذ إجراءات سريعة، لأن الدليل الرقمي غير مادي ويمكن التخلص من أية أدلة أو آثار من قبل مرتكبي الجرائم المعلوماتية، ولاشك أن الأجهزة الأمنية تلعب دورا محوريا في عملية تنفيذ القانون والسهر على احترامه على الوجه الصحيح، وهي بذلك تحافظ على القيم الاجتماعية والاقتصادية والأخلاقية. والجرائم المعلوماتية باعتبارها من الجرائم المرتبطة بالتطور التكنولوجي فهي تلقي مزيدا من الأعباء على أجهزة الأمن وهذا يرجع بالأساس إلى قلة الخبرة الفنية، ومن جهة أخرى إلى قصور المنظومة التشريعية في هذا المجال، وهذا ما خلق عدة صعوبات حالت دون أداء هذه الأجهزة لدورها في مواجهة هذه الجرائم[2].

الفرع الثاني: الصعوبات المتعلقة بجهات التحقيق

تتعلق هذه الصعوبات بالعامل البشري القائم بالتحقيق في الجريمة المعلوماتية بسبب نقص الخبرة لدى المحقق، وأجهزة العدالة الجنائية، وذلك فيما يتعلق بثقافة الحاسب الآلي وكيفية

1- خالد عياد الحلبي، مرجع سابق، ص 220.

2- السراني، عبد الله بن سعود، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم المنية، الرياض، 2009، ص65.

التعامل معها، وهذا ما يلاحظه جانب كبير من الفقه الجنائي، ذلك أن البحث والتحقيق في الجريمة المعلوماتية هي مسألة في غاية الأهمية والصعوبة، ولا سيما بالنظر لاعتبارات التكوين العلمي والتدريبي والخبرات المكتسبة لرجال الضبط القضائي وسلطات التحقيق الجنائي، ذلك أن هذه الجريمة تتقدم بسرعة هائلة توازي سرعة تقدم تقنياتها، مما يتطلب من القائمين على البحث الجنائي والتحقيق إلمام كافي لها، فلا يكفي أن يكون لديهم الخلفية القانونية أو أركان العمل الشرطي فقط ولكن لابد من اكتساب خبرة فنية في مجال الجرائم المعلوماتية عن طريق الحاسب الآلي[1].

المطلب الثاني: صعوبات الدليل الرقمي في إثبات الجريمة المعلوماتية

إن الطبيعة غير المادية للبيانات المخزونة بالحاسب الآلي والطبيعة المعنوية لوسائل نقل هذه البيانات تثير مشكلات عديدة في الإثبات الجنائي ويكون الدليل الرقمي الناتج عن الجرائم التي تقع على العمليات المعلوماتية غاية في الصعوبة كما أن الكم الهائل للبيانات التي يجري تداولها في الأنظمة المعلوماتية تشكل أحد الصعوبات التي تعوق التحقيق في الجرائم التي تقع عليها[2].

الفرع الأول: مظاهر الصعوبة في إثبات هذا النوع من الجرائم

1- غياب الدليل المرئي للجرائم التي تقع على العمليات المعلوماتية المختلفة والممكن بالقراءة فهمه، إذ إن مرتكبي هذا النوع من الجرائم نادرا ما يتركون آثارا مادية ملموسة يمكن أن تشكل طرف خيط يقود إليهم بفضل مهاراتهم في استخدام هذه التقنيات وبرامجها.
2- سهولة محو الدليل الرقمي أو تدميره في زمن قصير، فالجاني يمكنه محو الأدلة التي تكون قائمة ضده أو تدميرها في زمن قصير جداً، بحيث يصعب على الجهات التحقيقية كشف الجريمة إذا علمت بها، وفي الحالة التي قد تعلم بها فإن المجرم يستهدف بالمحو السريع لعدم استطاعة السلطات إقامة دليل ضده.
3- صعوبة الوصول إلى الدليل الرقمي لإحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم تمنع الوصول إليها أو تشفيرها لإعاقة المحاولات الرامية إلى الوصول إليها والإطلاع على محتواها أو استنساخها، كذلك فإن مرتكبي جرائم الإنترنت يصعب

[1]- عبد المطلب، ممدوح عبد الحميد، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، دار الحقوق، الشارقة، 2001، ص20.

[2] - http://pulpit.alwatanvoice.com/articles/17-09-2018.html.

ملاحقتهم لاستحالة تحديد هويتهم سواء عند قيامهم ببث المعلومات على الشبكة أو عند تلقيهم لها.

4- صعوبة فهم الدليل الرقمي المتحصل من عمليات فنية معقدة والتي تكون عن طريق التلاعب في نبضات وذبذبات الكترونية الوسائل المعلوماتية، ذلك لأن أغلب البيانات والمعلومات التي يتم تداولها عبر الحاسب الآلي وشبكة الانترنت هي عبارة عن رموز مخزنة على وسائط ممغنطة لا يُمكن الوصول إليها إلا بواسطة الحاسب الآلي ومن قبل أشخاص قادرين على التعامل مع هذه الأجهزة ونظمها[1].

الفرع الثاني: مشروعية وجود والحصول على الدليل الرقمي

1- **مشروعية وجود الدليل الرقمي:** يقصد بمشروعية وجود الدليل الرقمي أن يعترف المشرع بهذا الدليل من خلال تصنيفه في قائمة الأدلة القانونية التي يجيز القانون فيها القاضي الاستناد إليه في تكوين عقيدته، ولعل المعيار الذي يتحدد على أساسه موقف القوانين فيما يتعلق بسلطة القاضي الجزائي في قبول الدليل الرقمي يتمثل في طبيعة نظام الإثبات السائد في الدولة، إذ تختلف النظم القانونية في موقفها من حيث الأدلة التي يمكن قبولها في الإثبات.

وفي هذا الصدد فإن المشرع الجزائري وكغيره من التشريعات المنتمية إلى نظام الإثبات الحر لا نجده قد أفرد نصوصا خاصة تحظر على القاضي مقدما قبول أو عدم قبول أي دليل بما في ذلك الدليل الرقمي، وهنا يكون الدليل الرقمي مشروعا من حيث الوجود لأن الأصل في الأدلة هو مشروعية وجودها ومن جهة أخرى فإنه وطبقا لمبدأ الشرعية الإجرائية فلا يكون الدليل مقبولا في عملية الإثبات إلا إذا كان مشروعا بمعنى أنه تم البحث عنه والحصول عليه وفقا لطرق مشروعة[2].

2- **مشروعية الحصول على الدليل الرقمي:** إنه من المقرر الإدانة في أي جريمة لابد وأن تكون مبنية على أدلة مشروعة، ولا تكون كذلك إلا إذا أجري التنقيب عنها والحصول عليها أو كانت

1- راشد بشير إبراهيم، التحقيق الجنائي في جرائم تقنية المعلومات (دراسة تطبيقية على إمارة أبو ظبي)، بحث منشور في مجلة دراسات إستراتيجية، مركز الإمارات الدراسات والبحوث الإستراتيجية، العدد 131، 2008، ص 90.

2- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، باتنة، 2013، ص208-210

عملية تقديمها إلى القضاء أو إقامتها أمامه بالطرق التي رسمها القانون، وعلى هذا الأساس فإن إجراءات جمع الأدلة الرقمية المتحصلة من الوسائل المعلوماتية إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها فإنها تكون باطلة، وبالتالي بطلان الدليل.

والحقيقة أن مشروعية الدليل تعد قيدا وخطا فاصلا بين حق الدولة في توقيع العقاب لضمان أمن واستقرار المجتمع من جهة، وبين ضمان حقوق الأفراد وحرياتهم من جهة أخرى.

الخاتمة

إن محاربة الجريمة المعلوماتية سواء على المستوى الدولي أو الوطني لا يستقيم إلا بإيجاد أساس تشريعي موحد وتصور شامل لمفهوم هذه الجريمة من أجل تحديد الأفعال التي تشكل جريمة معلوماتية إضافة إلى عقد اتفاقيات سواء ثنائية أو جماعية يكون هدفها تنسيق وتوحيد الجهود قصد محاربة الجريمة وتشكيل لجان متخصصة في البحث والتحقيق والتحري يكون أعضاؤها ذوي كفاءات عالية في المجال المعلوماتي، والتعامل مع المعلومة الالكترونية. فهذا التنسيق والانسجام لا تمكن له أن يقوم إلا على ملائمة التشريعات الوطنية والاتفاقات الدولية في مجال مكافحة الجريمة المعلوماتية في إطار التعاون الدولي الجاد والمثمر. وعليه تم التوصل إلى النتائج والتوصيات التالية:

النتائج والتوصيات:

1) النتائج:

- تتسم الجريمة المعلوماتية بصعوبة اكتشافها، حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم قليلة إذا قورنت بم يتم اكتشافه من الجرائم التقليدية ويمكن رد الأسباب التي تقف وراء هذه الصعوبة في اكتشاف الجريمة المعلوماتية إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية، كما أن الجاني يمكنه ارتكاب هذه الجريمة في دول وقارات أخرى، إذ أن هذه الجريمة المعلوماتية جريمة عابرة للدول (دولية).
- بعد الإثبات من أهم التحديات التي تواجه الأجهزة الأمنية، ويزداد الإثبات صعوبة في الجريمة المعلوماتية، حيث أن اكتشاف هذه الأخيرة أمر ليس بالسهل، وفي حال اكتشافها والإبلاغ عنها فإن إثباتها أمر يحيط به كثير من الصعاب مما يستلزم الكثير من الجهد والخبرة الفنية.
- تواجه طرق التحقيق في إثبات الجريمة المعلوماتية صعوبات متعددة، حيث تستدعي هذه الطرق في المقام الأول اكتشاف الجريمة المعلوماتية، ومحلها، وبيئتها، ومن ثم البلاغ عنها، وأخذ

إذن الجهات المختصة قبل القيام بالمعاينة والتفتيش للموقع أو الجهاز المشتبه به، وذلك للبحث عن الدليل الرقمي الالكتروني بالطرق الفنية، ومن ثم إجراء التحريات، التي تساعد في عملية الإثبات.

- يعتبر فقدان الأثر من أهم المعوقات التي تواجه إثبات الجرائم، حيث تظل الجرائم المعلوماتية عن طريق الحاسب الآلي مجهولة ما لم يبلغ عنها الجهات الخاصة بالاستدلالات أو التحقيق الجنائي، والمشكلة التي تواجه أجهزة العدالة الجنائية أن هذه الجرائم لا تصل لعلم السلطات المعنية بطريقة اعتيادية كباقي جرائم قانون العقوبات، فهي جرائم غير تقليدية، لا تخلف آثارا مادية كتلك التي تخلفها الجريمة العادية.

- إن الدليل الرقمي على ضوء ما أسفرت عليه التطورات التقنية في مجال المعلوماتية لا يغني عنه أن يكون مشروعا، وذلك بأن يتم الحصول عليه بالطرق القانونية وأن يقدم للمحكمة على نفس الهيئة التي تم جمعه عليها، بأن لا يطرأ عليه أي تغيير أو تحريف خلال فترة حفظه.

2) **التوصيات:**

- زيادة الاهتمام بتدريب الكوادر والاستعانة بالخبرة الفنية، حيث تستدعي عملية التحقيق في مجال الجرائم المعلوماتية وأن يتم تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلاءم مع هذه الخصوصية، وتمكن رجال الشرطة، والمحقق من كشف الجريمة، والتعرف على مرتكبيها بالسرعة والدقة اللازمة لذلك. ولتحقيق ذلك يجب تدريب الكوادر التي تباشر التحريات والتحقيقات مع الاستعانة بذوي الخبرة الفنية المتميزة في هذا المجال.

- أهمية إنشاء أقسام أو إدارات في جهات الضبط الجنائي والتحقيق متخصصة في مجال الجريمة المعلوماتية، ويكون من ضمن اختصاصاتها متابعة ما يستجد من تطورات في مجال التقنية الحديثة للتعامل مع الجرائم المستحدثة في هذا المجال.

- التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة، أو المحافظة على دعاماتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على دعائمها الممغنطة.

الآليات المستحدثة لإثبات الجريمة المعلوماتية

The mechanisms developed to prove information crime

د. بوزوينة محمد ياسين

كلية الحقوق و العلوم السياسية

جامعة أبو بكر بلقايد – تلمسان الجزائر

مقدمة :

إن الأهداف التي يسعى القضاء إلى تحقيقها هو إقامة العدل بين الناس وذلك عن طريق إعطاء لكل ذي حق حقه ، وإنصاف المظلوم ، فهو يبذل مجهودات كبيرة من أجل تحقيقها ، فالقاضي هو الذي أنيطت له المهمة، حيث أنه يتحرى وجه الحق في الدعوى من البيانات المعروضة عليه ، فيقوم بمحصها واختيار الأقرب منها للحقيقة ،ولهذا السبب فقد اعتبر الإثبات من أهم وأعقد المواضيع في القانون الجنائي.

ونظرا للتطور التكنولوجي الذي يشهده عصرنا ، فإن العلم الحديث يعمل على مسايرته وذلك بوضع وسائل علمية تماشي مع هذا العصر ،وقد جاءت هذه الأخيرة من أجل سد العجز الذي يكتنف الأدلة الكلاسيكية والتي تعتمد على أدلة بسيطة للكشف عن مختلف الجرائم كالإعتراف والشهادة ، إلا أن المجرم في الجرائم التقنية يلجأ إلى مختلف الوسائل العلمية من أجل تنفيذ سلوكه الإجرامي وتحقيق هدفه المنشود مما يصعب على السلطات المختصة التعرف على هوية الجناة ، الأمر الذي أدى بهذه السلطات إلى اللجوء إلى تلك الأساليب حتى يتسنى لها الوصول إلى الحقيقة دون أي شيب أو عيب ،وذلك لأن الوسائل العلمية الحديثة تصل إلى حد اليقين .

ونظرا لإهمية الإثبات الجنائي في مجال الجرائم المعلوماتية فقد كان محور دراستنا في هذا البحث ، وتكمن هذه الأهمية في كون أن الجرائم المعلوماتية المستحدثة والتي في تطور مستمر كما أن أساليب ارتكابها دائمة العمل على مواكبة التطور التكنولوجي الحاصل في ميدان المعلوماتية، لذلك فإن هذا النوع من الجرائم يرتبط من المستجدات التي لم تكن معروفة في مجال القانون الجنائي سواء من الناحية الموضوعية أو الإجرائية، بالإضافة إلى ذلك فإن أهمية هذا الموضوع تتضح في كونه تناول أحدث الوسائل العلمية وأكثرها انتشارا في قضايا الإثبات الجنائي ألا وهو الدليل الإلكتروني والذي جاء ليتلاءم مع التطورات التكنولوجية، كما أنه ومن دون منازع فإن أي محاولة للتعامل إجرائيا مع هذا النوع من الأدلة في إطار عملية البحث والتحري سبب عدة

إشكالات إجرائية للأجهزة المكلفة لهذه العملية ،وينبغي أن تأتي الدراسات القانونية من أجل الشرح والإيضاح لذلك .

أما بالنسبة لإشكالية الموضوع ، فباعتبار أن الجريمة الإلكترونية من الجرائم المستحدثة المتعلقة بالكيانات غير المادية، مما يؤكد على صعوبة الكشف عنها واثباتها ، وهذا راجع للطبيعة الخاصة والمعقدة للدليل الإلكتروني، وذلك لأن مستودع هذه الأدلة هو الوسائل الإلكترونية مما يجعلها قابلة للتلاعب والتغيير في الحقيقة التي وجدت من أجل التعبير عنها، وعلى هذا الأساس ارتأينا بأن تكون اشكالية دراستنا كالأتي: فيما تمثل أدلة إثبات وجمع الجريمة المعلوماتية الحديثة؟

المبحث الأول: الدليل الإلكتروني

إن الجرائم الإلكترونية ذات طبيعة خاصة ،لذا فإن الكشف عن هذا النوع يحتاج إلى أدلة تعيش في العالم الافتراضي ،حيث تستخدم فيها الطبيعة التقنية وتمثل في الدليل الإلكتروني، ويعد الوسيلة الوحيدة للإثبات في هذه الجرائم ، لذلك فستكون محور دراستنا تمثل في تعريف الدليل الإلكتروني ، ثم نتطرق إلى خصائص الدليل الإلكتروني ، ثم نتناول أنواع الدليل الإلكتروني.

المطلب الأول: تعريف الدليل الإلكتروني .

عرف الدليل الإلكتروني بأنه : **" الدليل الذي يجد له أساسا في العالم الإفتراضي ويقود إلى الجريمة، فهو الجزء المؤسس على الإستعانة بتقنية المعالجة التقنية للمعلومات ،والذي يؤدي إلى اقتناع قاضي الموضوع بثبوت ارتكاب شخص ما لجريمة عبر الأنترنت "**[1]

كما عرف كذلك بأنه: **" معلومات يقبلها العقل والمنطق ويعتمدها العلم ، يتم الحصول عليها بإجراءات علمية وقانونية بترجمة المعلومات والبيانات المخزنة في الحاسوب وملحقاته وشبكات الإتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق والمحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بالجريمة[2] ".**

[1]- فتحي محمد أنور عزت ، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية ، دار الفكر والقانون ، مصر ، 2010، ص 235.

[2]- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت ، الطبعة الأولى ، دار الثقافة للنشر والتوزيع ، عمان، 2011 ، ص 230.

وقد عرفه البعض بأنه : " **جميع البيانات الرقمية التي يمكن أن تثبت أن هناك جريمة قد ارتكبت ، أو توجد العلاقة بين الجريمة والجاني ،أو توجد العلاقة بين الجريمة والمتضرر**"[1].

وعرف كذلك بأنه : " **كل البيانات التي يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسوب من إنجاز مهمة ما** " [2].

ويعود سبب تسميته بهذا الإسم كون أن البيانات الموجودة داخل نظام الحاسب الآلي سواء كانت كتابات أو صور أو رسومات أو نصوص ، فإنها تكون في شكل أرقام المتمثلة في الرقمين (0،1) ليقوم هذا النظام بتحويل ومعالجة هذه الأرقام لتظهر عند عرضها في شكل مسند أو صورة ، كما أنه يتم الحصول على هذا الدليل عن طريق مخرجات الطابعة على الورق كالتقارير والرسومات والأقراص الصلبة والمرنة وأشرطة تخزين المعلومات ، وكل هته تكون في أجهزة الكمبيوتر وملحقاته ، أو في أجهزة الاتصال كالمواقع الالكترونية والبريد الالكتروني وأجهزة التصوير كآلة التصوير الرقمية [3].

من خلال التعاريف السابقة يتضح لنا أن هناك من ألحق تعريف الدليل الإلكتروني بتعريف برامج الحاسوب الآلي رغم الإختلاف بينهما والذي يكمن في الوظيفة التي يؤديها كل واحد منها ، فللدليل الإلكتروني دور أساسي في معرفة كيفية وقوع جرائم الإعتداء على النظم المعلوماتية بهدف إثباتها ونسبتها إلى مرتكبيها ،أما بالنسبة

لبرامج الحاسوب فإن أهميتها تجلى بوضوح في العمليات التي تقوم بها داخل الحاسب الآلي كتشغيله وتوجيهه إلى حل المشاكل ووضع الخطط المناسبة ، فبدونها يصبح الحاسب مجرد آلة صماء كغيره من الآلات[4].

المطلب الثاني : خصائص الدليل الإلكتروني.

---

[1]- رشيدة بوبكر ، جرائم الإعتداء على نظم المعالجة الآلية ، الطبعة الأولى ، منشورات الحلبي القانونية ، لبنان ، 2012، ص 383.

[2]- أشرف عبد القادر قنديل ، الإثبات الجنائي في الجرائم الإلكترونية، دار الجامعة العربية ، مصر ، 2015، ص 123.

[3]- عبد القادر معتوق ،الإطار القانوني لمكافحة الجريمة المعلوماتية في التشريع الجزائري والتشريع المقارن ،مذكرة ماجستير ، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر ، باتنة ، 2012، ص 118.

[4]- أشرف عبد القادر قنديل ، المرجع السابق ، ص 124.

إن البيئة الإفتراضية التي يعيش فيها الدليل الإلكتروني قد انعكست على طبيعة هذا الأخير، مما جعله يتصف بعدة صفات وخصائص تميزه عن غيره من الأدلة ، سنتطرق فيما يلي أهم هذه الخصائص والتي سيأتي بيانها كالآتي:

الفرع الأول : الدليل الإلكتروني دليل علمي.

يتكون الدليل الإلكتروني من بيانات ومعلومات ذات صفة الكترونية غير ملموسة وتدرك بالحواس العادية ، بل يتطلب إدراكها الإستعانة بالحاسوب والأجهزة الالكترونية باستخدام برامج الكترونية خاصة بذلك[1]، بمعنى الحصول أو الإطلاع على الدليل الالكتروني لا يكون إلا بإستخدام الأساليب العلمية ، وأن رجال الضبط القضائي والإستدلال أو سلطات التحقيق لا تبني عملية بحثها إلا عن طريق أسس علمية ، وأن الدليل العلمي يخضع لقاعدة لزوم تجارية مع الحقيقة كاملة ،وهذا وفقا للقاعدة " **أن القانون مسعاه العدالة ، أما العلم فسعاه الحقيق**"[2]، فالدليل العلمي لا يمكن تعارضه مع القواعد العلمية السليمة بمعنى أن لهذا الأخير منطقة محددة لا يمكنه الخروج عن تلك الحدود، فضلا عن ذلك فإن للدليل الإلكتروني نفس الطبيعة ، فلا يمكنه أن يخرج هذا النوع من الأدلة عما توصل إليه العلم الإلكتروني ،وإلا فقد معناه ، بمعنى أن ما ينطبق على الدليل العلمي ينطبق على الدليل الإلكتروني[3].

الفرع الثاني : الدليل الإلكتروني دليل تقني .

إن التقنية مبنية على أسس علمية ،فيما أن الدليل الإلكتروني هو دليل علمي ، فإن التقنية تعد أحد الخصائص التي يمتع بها هذا الأخير بحيث أن التعامل مع الدليل الإلكتروني يكون من طرف تقنيين مختصين في العالم الإفتراضي ، فلا يمكن أن تنتج التقنية سكينا يتم به اكتشاف القاتل أو إعترافا مكتوبا ، كما هو الحال بالنسبة للأدلة العادية ، وإنما تنتج التقنية نبضات رقمية تصل إلى درجة خيالية في شكلها وحجمها ومكان تواجدها، فهي ذات طبيعة ديناميكية فائقة السرعة[4].

وبفضل الطبيعة التقنية للدليل الإلكتروني فإنه قد اتصف بصفات تميزه عن الدليل المادي ،خاصة من ناحية قابليته للنسخ، بحيث يمكن استخراج نسخ مطابقة للأصل من الأدلة

---

[1]- خالد عياد الحلبي ، المرجع السابق ، ص 231.

[2]- فتحي محمد أنور عزت ، المرجع السابق ، ص 648.

[3]- رشيدة بوبكر ، المرجع السابق ، ص 387.

[4]- فتحي محمد أنور عزت ، المرجع السابق ، ص 649.

الإلكترونية ، وتكون لها نفس القيمة العلمية، وهذه الميزة لا يمكن أن تتوافر في الأدلة الأخرى، فبفضل ذلك يمكن تحديدها إذا تم العبث بالدليل الإلكتروني أو تعديله وذلك من خلال القيام بمقارنته بالأصل عن طريق استخدام البرامج والتقنيات الصحيحة ، بالإضافة إلى ذلك فإنه يشكل ضمانة شديدة الفعالية للحفاظ عليها من التعرض للإتلاف[1]، ضف إلى ذلك فإن الدليل الالكتروني لا يخضع لقواعد التفسير والتأويل كما هو الحال في الدليل المادي ، والذي يحتاج إلى فترة زمنية طويلة لإرساء فهم لها ، بل يحتاج إلى تفاعل التقنية مع ذاتها فقط[2].

الفرع الثالث : الدليل الإلكتروني يصعب التخلص منه.

إن هذه الخاصية من أهم الخصائص التي يتمتع بها الدليل الإلكتروني عن غيره من الأدلة التقليدية، وهذه الأخيرة يمكن التخلص منها بطرق سهلة وبسيطة كتمزيق وحرق الأوراق والأشرطة المسجلة التي تحمل إقرارا بإرتكاب الشخص لإحدى الجرائم ، ويمكن التخلص منها من بصمات الأصابع بمسحها من مكان تواجدها، كما أنه قد يلجأ بعض المشتبه فيهم إلى قتل الشهود أو تهديدهم بعدم الإدلاء بالشهادة ...إلخ.

حيث أنه من الصعب استرجاع أو استرداد الدليل المستمد منها، وذلك بسبب قيامهم بتدميرها نهائيا على عكس الدليل الالكتروني الذي يمكن استرجاعه بعد محوه وإصلاحه ، بعد إتلافه وإظهاره بعد إخفاءه الأمر الذي يؤدي إلى صعوبة التخلص منه ،وهذا راجع إلى مختلف البرمجيات الرقمية التي يمكن بواسطتها استرجاع جميع الملفات التي تم إلغاءها وإزالتها[3] ،والسبب في ذلك كون أن المساحة التي يشغلها الملف تبقى كما هي متاحة إن لم يتم شغلها بملف آخر[4].

فضلا عما سبق فإن ما يتم استخلاصه هو أن هذه الخاصية نتج عنها مسائل قانونية هامة أبرزها مسألة التخلص أو إخفاء الدليل، فإذا ثبت أن الجاني في الجريمة الالكترونية قد قام باستخدام البرمجيات من أجل التخلص من الدليل، فإن يعرض للإدانة وذلك وفقا للنصوص القانونية التي تجرم مثل هذه السلوكات[5].

الفرع الرابع : الدليل الإلكتروني ذو طبيعة رقمية ثنائية.

---

[1]- نعيم سعيداني ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة ماجستير ، كلية الحقوق والعلوم السياسية ، جامعة الحاج لخضر ، باتنة ، ص 123.

[2]- فتحي محمد أنور عزت ، المرجع السابق ، ص 651.

[3]- رشيدة بوبكر ، المرجع السابق ، ص 388.

[4]- فتحي محمد أنور عزت ، المرجع السابق ، ص 655.

[5]- نعيم سعيداني ، المرجع السابق ، ص 125.

إن الدليل الالكتروني يتميز بخاصية الالتصاق بمفهوم تكنولوجيا المعلومات من حيث تكوينه ، إذ لا يمكن أن يكون على هيئة واحدة ،فهو يتكون من عدد غير محدود من الأرقام الثنائية الموحدة المكونة من الرقمين (0،1) والتي تميز بعدم تشابهها على الرغم من وحدة الرقم الثنائي الذي يتكون منه، فنذكر على سبيل المثال الكتابة في العالم الإفتراضي ليس لها الوجود المادي المعروف الذي يكون في شكل ورقي، وإنما هي عبارة عن الأرقام التي ترجع أصل واحد وهو الرقم الثنائي ، فأي عملية يقوم بها مستخدم النظام المعلوماتي تكون عبارة عن الرقمين صفر وواحد (0،1) ،فهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها من الطاقة، وأن كمية الرقمين (0،1) تختلف من ملف لآخر ،وذلك حسب حجم كل واحد منهم[1].

وقد جعلت هذه الخاصية للدليل الالكتروني طابعا متميزا فأصبح الدليل الأصل للإثبات في الجرائم الإلكترونية، وذلك لأنه ينتمي إلى نفس البيئة التي ارتكبت فيه ألا وهي البيئة الرقمية، سواء أكانت هذه الجرائم مرتكبة بواسطة نظام المعالجة الآلية كغسيل الأموال أو تهريب المخدرات الكترونيا ، أو الإعتداء على نظم المعالجة الآلية[2].

الفرع الخامس : الدليل الإلكتروني دليل متنوع ومتطور.

إن الدليل الإلكتروني يشمل جميع أنواع البيانات الرقمية التي يمكن تداولها الكترونيا ، وتعني هذه الخاصية بأنه على الرغم من أن تكوين الدليل الالكتروني يعتمد على لغة الحوسبة والرقمنة ، إلا أنه يتخذ أشكالا مختلفة كأن يكون في شكل بيانات غير مقروءة، كما هو الحال في المراقبة عبر الشبكات ، وقد يكون عبارة عن بيانات مقروءة كالوثيقة المعدة بنظام المعالجة الآلية ، بالإضافة إلى ذلك يمكن أن يكون عبارة عن صورة ثابتة أو متحركة أو مخزنة في البريد الإلكتروني ،وبهذا نستنتج أن الدليل الإلكتروني يشمل أنواعا متعددة من البيانات الرقمية والتي تصلح بأن تكون دليل إدانة أو براءة[3].

المطلب الثالث : أنواع الدليل الإلكتروني.

إن الجرائم الإلكترونية تتم في بيئة غير مادية ، فتكون عبر أنظمة المعالجة الآلية ، وبذلك يتمكن الجاني من العبث ببيانات الحاسب الآلي وببرامجه في فترة زمنية وجيزة ، ويمكنه من

1- رشيدة بوبكر ، المرجع السابق ، ص 390.

2- نعيم سعيداني ، المرجع السابق ، ص 126.

3- نعيم سعيداني ، المرجع نفسه ، ص 124.

طمسها ومحوها في وقت قياسي ،مما نتج عنه أدلة إثبات مختلفة ذات طبيعة الكترونية ،وقد قسمت الأدلة الالكترونية إلى قسمين ، فالأول يتمثل في الأدلة التي أعدت لتكون وسيلة إثبات، والثاني الأدلة التي لم تعد لتكون وسيلة إثبات.

الفرع الأول : الأدلة التي أعدت لتكون وسيلة إثبات:

تمثل هذه الأدلة في:

أولا: السجلات التي تم إنشاءها بواسطة الجهاز تلقائيا : وتمثل هذه السجلات في مخرجات الحاسوب التي لم يكن للأفراد يد في إنشائها ،وكأمثلة عن ذلك الهواتف ، البطاقات البنكية ، والفواتير.

ثانيا : السجلات التي تم حفظ جزء منها والجزء الأخر تم إنشاؤه بواسطة الحاسب الآلي: وكمثال عن ذلك رسائل غرف المحادثة المتبادلة عبر الأنترنت.

الفرع الثاني: الأدلة التي لم تعد لتكون وسيلة إثبات.

وقد أنشأ هذا النوع من الأدلة دون إرادة الفرد ، فهي عبارة عن أثار يتركها الجاني في مسرح الجريمة دون رغبته في وجودها ،ويطلق عليها تسمية البصمة الوراثية ، ويمكن تسميتها أيضا بالأثار المعلوماتية والرقمية، حيث أن هذا النوع من الأدلة لم يعد للحفظ ،لكن الوسائل الفنية الخاصة تمكنت من ضبط هذه الأدلة حتى وإن مرت عليها فترة زمنية طويلة ،وكأمثلة عن ذلك الإتصالات التي تم عبر الأنترنت والمراسلات التي صدرت من الجاني أو تلقاها[1].

المبحث الثاني: الإجراءات الحديثة لجمع الدليل الإلكتروني.

بالرجوع إلى الإجراءات التقليدية لجمع الدليل الإلكتروني يتضح أنها غير كافية لإثبات الجرائم الإلكترونية، وذلك نظرا للتعقيد والصعوبات التي تواجه السلطات المختصة أثناء استخلاصه ، الأمر الذي سهل على الكثير من المجرمين الإفلات من العقاب ،وعلى ذلك فقد كان من الضروري العمل على مواكبة هذا التطور التكنولوجي ،وهذا من خلال وضع طرق إجرائية حديثة تتناسب مع الطبيعة التقنية للجريمة الإلكترونية والدليل التقني الذي يصلح لإثباتها.

ولذلك سنتطرق إلى في هذا المطلب إلى الإجراءات الحديثة لجمع الدليل الإلكتروني بحثي سنتطرق لعملية التسرب ، وإعتراض المراسلات السلكية واللاسلكية ، وفي الأخير سنتناول إلى إجراء حفظ المعطيات المتعلقة بحركة السير .

المطلب الأول : عملية التسرب.

---

[1]- خالد عياد الحلبي ، المرجع السابق ، ص 234.

إن الجريمة الإلكترونية من الجرائم التي خصص لها المشرع إجراءات حديثة لجمع دليلها التقني ومن بينها إجراء التسرب والذي يتم اللجوء إليه إذا اقتضت ضروريات التحري أو التحقيق بذلك.

الفرع الأول : مفهوم عملية التسرب.

يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية بمراقبة الأشخاص المشتبه فيهم عن طريق التوغل داخل جماعاتهم الإجرامية ، وذلك بإيهامهم بأنه فاعل أو شريك معهم من أجل الكشف عن أنشطتهم، وتتم هذه العملية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب[1].

كما أن المشرع الجزائري قد عرف عملية التسرب في نص المادة 65 مكرر 12 من قانون الإجراءات الجزائية بأنها:" قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف[2] ".

تتم عملية التسرب في الجرائم الإلكترونية بدخول ضابط الشرطة القضائية إلى العالم الإفتراضي كاشتراكه في محادثات غرف الدردشة أو حلقات النقاش التي تدور حول قيام أحدهم باختراق الشبكات أو بث الفيروسات ، ويكون ذلك باتخاذ المتسرب لأسماء مستعارة وهمية متظاهرا بأنه فاعل مثلهم ، وذلك من أجل الوصول إلى الغاية التي رسمت لهذه العملية معرفة كيفية اقتحام الهاكر لموقع ما[3].

الفرع الثاني: شروط عملية التسرب.

لقد وضع المشرع الجزائري مجموعة من الشروط الشكلية والموضوعية لإجراء عملية التسرب، ويجب على ضابط أو عون الشرطة القضائية التقيد والتزام بها ، وإلا عد إجراءه باطلا.

البند الأول : الشروط الشكلية

---

[1]- عز الدين وداعي ، التسرب كأسلوب من اساليب البحث والتحري الخاصة على ضوء قانون الإجراءات الجزائية الجزائري والمقارن، المجلة الأكاديمية للباحث القانوني ، جامعة الحاج لخضر ، باتنة ، المجلد 16 ، العدد 02، 2017 ، ص 204.

[2]- الأمر 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية الجزائرية، العدد 49 ، الصادرة بتاريخ 11 جوان 1966 المعدل و المتمم.

[3]- رشيدة بوبكر ، المرجع السابق ، ص 434.

لمباشرة إجراء التسرب لابد من أن يصدر بإذن من وكيل الجمهورية أو قاضي التحقيق ،فلا يمكن لضابط الشرطة القضائية القيام بهذه العملية من تلقاء نفسه ، بل يجب عليه المرور الجهاز القضائي ، وذلك من أجل حماية الحقوق الأساسية للمتهم والمكرسة له دستوريا.

كما أن المشرع الجزائري اشترط لصحة هذا الإجراء أن يكون بإذن مكتوبا ، وذلك لأن الأصل في العمل الإجرائي أن يكون مكتوبا وإلا كان الإجراء باطلا [1]،وهذا وفقا لنص المادة 65 مكرر 15 من قانون الإجراءات الجزائية ،والتي جاء في فحواها " **يجب أن يكون الإذن المسلم طبقا للمادة 65 مكرر 11 أعلاه مكتوبا و مسببا وذلك تحت طائلة البطلان** [2]".

بالإضافة إلى ذلك فقد حددت المادة 65 مكرر 15 فقرة 03 من قانون الإجراءات الجزائية مدة التسرب بأن لا تجاوز 4 أشهر ، ويمكن أن تجدد بحسب مقتضيات التحري والتحقيق، على أن تخضع لنفس الشروط الشكلية والزمنية التي خضعت لها الفترة الأولى، كما أجاز المشرع الجزائري للقاضي الذي رخص بإجرائها أن يأمر بوقفها في أي وقت حتى وإن لم تنتهي المدة التي حددت هذا الإجراء.

كما أنه يتم إبقاء الإذن بالتسرب خارج ملف الإجراءات إلى غاية الإنتهاء من العملية ، وذلك من أجل الحفاظ على السرية المطلوبة بين القاضي وضابط الشرطة القضائية المشرف على عملية التسرب، ضف إلى ذلك فإنه يشترط وجود تقرير مسبق محرر من طرف ضابط الشرطة القضائية ، ويكون ذلك بشكل مفصل من أجل اطلاع القاضي على ظروف العملية ومتطلباتها.

البند الثاني : الشروط الموضوعية.

تتمثل الشروط الموضوعية لصحة عملية التسرب في شرطين أساسيين:

- **فالشرط الأول يتمثل في تحديد نوع الجريمة:** والتي ذكرها المشرع الجزائري على سبيل الحصر ، فلا يمكن أن تخرج عن الجرائم التي حددتها المادة 65 مكرر 05 من قانون الإجراءات الجزائية ، وهي سبعة أنواع تتمثل في جرائم المخدرات ، الجريمة المنظمة العابرة للوطنية ، جرائم تبييض الأموال ، الجرائم الإرهابية ، جرائم الفساد ،الجرائم المتعلقة

---

[1]- فضيل يعيش ، شرح قانون الإجراءات الجزائية بين النظري والعملي ، مطبعة البدر ، الجزائر ، 2008 ، ص 130.

[2]- نص المادة 65 مكرر 15 من الأمر 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية.

بالتشريع الخاص بالصرف ، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، فلا يكون هذا الإجراء إلا في حدود هذه الجرائم وإلا عد باطلا[1].

- **أما بالنسبة للشرط الثاني فيجب أن يكون الإذن بالتسرب مسببا:** أي أن النيابة العامة تقوم بذكر المبررات التي أسندت إليها لإصداره والتي دفعت بضابط الشرطة القضائية بتنفيذ عملية التسرب من خلاله تبين العناصر التي اقنعت الجهات القضائية المختصة لمنح الإذن[2].

الفرع الثالث: أثار عملية التسرب.

إن صدور الإذن بالتسرب ومباشرة ضابط الشرطة القضائية لعمله حسب المقتضيات المطلوبة يترتب عنه آثار والمتمثلة في :

البند الأول : تسخير الوسائل المادية والقانونية :

لقد رخص المشرع الجزائري لضابط الشرطة القضائية بأن يقوم بمجموعة من الأفعال غير المشروعة أثناء ممارسته لعملية التسرب ،ويتضح ذلك في المادة 65 مكرر 14 من قانون الإجراءات الجزائية التي نصت على أنه: " يمكن لضابط أو عون الشرطة القضائية المرخص لهم بإجراء عملية التسرب والأشخاص الذين يسخرونهم لهذا الغرض دون أن يكونوا مسؤولين جزائيا القيام بما يلي :

- اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها
- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي ، وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الإتصال ".

ومن خلال نص هذه المادة يتبين أن القانون قد أخرج هذه الأفعال من دائرة التجريم وجعلها مباحة بالنسبة للمتسرب ، حيث يمكنه من تسخير جميع الوسائل المادية لتحقيق السلوك الإجرامي ، كالنقل أو التسليم أو التخريب ، كما أنه يعمل كذلك على تسخير وسائل قانونية ويكون ذلك بتوفير الوثائق الرسمية اللازمة كاستخراج بطاقة التعريف أو رخصة السياقة عن

[1]- نعيم سعيداني، المرجع السابق ، ص 176.
[2]-عز الدين وداعي ، المرجع السابق ، ص 210.

طريق جهاز خاص بتزوير الوثائق الرسمية ، وفي هذه الحالة لا يمر على الإدارة المختصة من أجل الإبقاء على سرية أعماله[1].

البند الثاني: إحاطة العملية بسرية تامة .

إن عملية التسرب تتطلب السرية التامة وهذا من أجل تحقيق الأهداف المراد الوصول إليها ،ولذلك فقد قرر المشرع الجزائري جزاءات عقابية مشددة للمتسرب الذي يكشف عن هويته الحقيقية[2] ،بحيث تتراوح هذه العقوبات من سنتين إلى 5 سنوات حبسا وبغرامة من 50 ألف إلى 200 ألف دج ، وهذا بموجب المادة 65 مكرر 16 من قانون الإجراءات الجزائية ، مما يفرض على المتسرب الإلتزام بالسرية التامة لمهامه[3].

البند الثالث : الإعفاء من المسؤولية .

إن طبيعة الأفعال المصرح بها للمتسرب تفرض عليه أن تكون مشاركته إيجابية لحيازة متحصلات الجريمة أو وسائل لارتكابها ، وأن هذا النوع من الأفعال له تأثير على المسؤولية الجزائية ،لذلك فقد قام المشرع بإعفائهم صراحة من هذه المسؤولية ، وهذا ما يتضح من نص المادة 65 مكرر 14 من قانون الإجراءات الجزائية ، بل وقد مد نطاق هذا الإعفاء لظروف أمنية للمتسرب حتى بعد المهلة المحددة له في الرخصة ، وفي حالة عدم تمديدها أو تقرير وقف العملية ، على أن لا يتجاوز ذلك 4 أشهر من تاريخ إنقضاء المدة المحددة في الإذن أو تاريخ صدور قرار وقفها من طرف القاضي الذي صرح بها[4].

وهذه الفكرة ما هي إلا تكريسا للمادة 39 الفقرة الأولى من قانون العقوبات التي نصت على أنه " لا جريمة إذا كان الفعل قد أمر أو أذن به القانون... "[5].

المطلب الثاني : إعتراض المراسلات السلكية واللاسلكية.

---

[1]- رشيدة بوبكر ، المرجع السابق ، ص 437.

[2]- عائشة بن قارة مصطفى ، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن ،دار الجامعة الجديدة ، الإسكندرية ، مصر ،2011، ص 123.

[3]- نص المادة 65 مكرر 16 من قانون الإجراءات الجزائية.

[4]- عبد الرحمان خلفي ،الإجراءات الجزائية في التشريع الجزائري والتشريع المقارن ، دار بلقيس ، الجزائر ، 2018، ص 100.

[5]- نص المادة 39 من الأمر 66-156 المؤرخ في 08 جوان 1966 المتضمن قانون العقوبات، الجريدة الرسمية الجزائرية ، العدد 49 ، الصادرة بتاريخ 11 جوان 1966 المعدل و المتمم.

يقوم ضابط الشرطة القضائية بمجموعة من الإجراءات لمراقبة أحد الأشخاص نتيجة للاشتباه في تصرفاته، ويكون ذلك بصورة خفية بحيث لا يحس الغير بمباشرتها ،وهذا نظرا لطابع السرية التي يكتنفها ، ومن بين هذه الإجراءات إعتراض المراسلات السلكية وهو ما تم إدراجه من طرف المشرع الجزائري في المواد (من 65 مكرر إلى 65 مكرر 10) من قانون الإجراءات الجزائية تحت عنوان في إعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

الفرع الأول: تعريف اعتراض المراسلات السلكية واللاسلكية .

يقصد باعتراض المراسلات السلكية واللاسلكية" عملية مراقبة سرية المراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم في إرتكابهم أو في مشاركتهم في إرتكاب الجريمة [1]".

كما عرفه البعض بأنه " إجراء خاص يقوم على التدخل الوسطي لتحويل مسار المراسلات في خط مشترك بوسيلة ممغنطة والقيام بنسخها[2] ".

أما المشرع الجزائري وبالرجوع إلى نص المادة 65 مكرر 5 ق إ ج فقد أجاز لضابط الشرطة القضائية اعتراض المراسلات التي تتم بواسطة وسائل الاتصال السلكية واللاسلكية بناء على إذن من وكيل الجمهورية أو قاضي التحقيق[3].

الفرع الثاني: الشروط المقررة لاعتراض المراسلات السلكية واللاسلكية

يخضع إجراء إعتراض المراسلات السلكية واللاسلكية لمجموعة من الشروط الموضوعية والإجرائية والتي سيأتي بيانها كالآتي:

البند الأول : الشروط الموضوعية.

لقد أجاز المشرع الجزائري عملية إجراء اعتراض المراسلات ولكن لا يكون ذلك إلا بتوافر مجموعة من الشروط الموضوعية والتي سيأتي بيانها كالآتي:

أولا: السلطة المختصة بإجراء هذه العملية

---

[1]- رشيدة بوبكر ، المرجع نفسه ، ص 441.

[2]- مريم مسعود ، آليات مكافحة جرائم تكنولوجيا الإعلام والإتصال في ضوء القانون 09-04 ، مذكرة ماجستير، كلية الحقوق والعلوم السياسية ، جامعة قاصدي مرباح ، ورقلة ، 2013 ، ص 81.

[3]-نصت المادة 65 مكرر 6 قانون الإجراءات الجزائية على أنه " يجوز لوكيل الجمهورية المختص أن يأذن بما يلي : اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ..".

إن السلطة القضائية هي المختصة بإصدار الإذن بها الإجراء، ويكون ذلك من طرف وكيل الجمهورية في مرحلة البحث والتحري في الجرائم المتلبس بها، ومن قاضي التحقيق المختص عند فتح التحقيق وهذا وفقا لأحكام المادتين 13 و 65 مكرر 5 في فقرتها الأخيرة من قانون الإجراءات الجزائية.

ويجب أن يوجه هذا الإذن لضابط الشرطة القضائية وليس لأعوانه ، وذلك لأن مهمتهم تنحصر في مساعدته ، كما أنه للضابط الحق في الإستعانة بالخبرة للتكفل بالجوانب التقنية لعملية المراقبة[1].

ولا يمكن منح هذا الإذن إلا بعد تقدير الفائدة من هذا الإجراء وجديته ومدى ملاءمته، وذلك بعد الإطلاع على معطيات التحريات التي قامت بها مصالح الضبطية القضائية مسبقا[2].

ثانيا : طبيعة الجريمة محل الاعتراض

لقد حدد المشرع الجزائري الجرائم التي يجوز إجراء عملية اعتراض السلكية واللاسلكية على سبيل الحصر،وهذا وفقا للمادة 65 مكرر 5 من قانون الإجراءات الجزائية والمتمثلة في جرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية ،والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال وجرائم الإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، وكذا جرائم الفساد، إلا أنه إن اكتشفت جرائم أخرى أثناء القيام بإجراءات التحري ولم تكن مذكورة في الإذن، فإن ذلك لا يكون سببا في بطلان الإجراءات العارضة ، وهذا وفقا للمادة 65 مكرر 6 من قانون الإجراءات الجزائية[3].

ثالثا : ميقات ومكان إجراء هذه العملية .

لم يضع المشرع الجزائري قيود لا زمنية ولا مكانية بإجراء عملية إعتراض المراسلات السلكية واللاسلكية ، وقد ترك الأمر للسلطات المختصة ، بحيث يمكنها القيام بهذا الإجراء في أي ساعة من ساعات الليل والنهار وفي أي مكان كان عاما أو خاصا[4].

البند الثاني : الشروط الإجرائية .

---

[1]- جميلة محلق ، إعتراض المراسلات ، تسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية ، مجلة التواصل في الاقتصاد والادارة والقانون ، جامعة باجي مختار ، عنابة ، العدد 42 ، 2015 ، ص 180.

[2]- رشيدة بوبكر ، المرجع السابق ، ص 444.

[3]- جميلة محلق ، المرجع السابق ، ص 179.

[4]- فوزي عمارة ، إعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراء تحقيق قضائي في المواد الجزائية ، مجلة العلوم الإنسانية، جامعة منتوري ، قسنطينة ، العدد 33 ، 2010 ، ص 239.

لقد قيد المشرع الجزائري إجراء اعتراض المراسلات السلكية واللاسلكية بمجموعة من الضوابط الإجرائية وتتمثل في :

أولا : شكل الإذن باعتراض المراسلات السلكية واللاسلكية

إن المشرع الجزائري لم يشترط شكلا معينا للإذن باعتراض المراسلات السلكية واللاسلكية، إلا أنه قد اشترط فيه أن يكون مكتوبا متضمنا لجميع العناصر التي تسمح لضابط الشرطة القضائية بالتعرف على الإتصالات المطلوب التقاطها والأماكن المقصودة، والجريمة التي يبرر اللجوء إليه، بالإضافة إلى ذلك فإن القانون قد حدد مدة القيام بهذه العملية ب 04 أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق ، وهذا من أجل الحد من التعسف في التعدي على حرمة الحياة الخاصة.

ثانيا : تحرير المحضر.

لقد ألزم المشرع الجزائري ضابط الشرطة القضائية بتحرير محضر يتضمن جميع الترتيبات المتعلقة بعملية اعتراض المراسلات، ويكون لكل عملية محضر منفصل على الأخر، ويذكر فيه تاريخ وساعة بداية وانتهاء هذه العمليات، والقيام بنسخها وترجمتها إن استلزم الأمر ذلك.

ثالثا : تنفيذ عمليات المراقبة

أثناء تنفيذ عمليات المراسلات السلكية واللاسلكية يلتزم ضابط الشرطة القضائية بكتمان السر المهني، وذلك باتخاذ التدابير اللازمة لاحترام ذلك السر من جهة، ومن جهة أخرى فقد سمح المشرع الجزائري لأعضاء الضبط القضائي بدخول المنازل لوضع أجهزة الاعتراض والتنصت دون التقيد بالزمن المحدد في المادة 27 من قانون الإجراءات الجزائية ذلك دون رضا وعلم صاحب المسكن[1].

المطلب الثالث: حفظ المعطيات المتعلقة بحركة السير.

يتسم الدليل التقني بخصائص مبنية على أساس الطبيعة المرنة التي يتميز بها العالم الافتراضي ، الأمر الذي يسهل على الفاعل إمكانية إزالته عن بعد باستخدام التقنية ذاتها ،فضلا عن ذلك فإن الفوضى التي تعم مؤسسات تقديم الخدمات الخاصة بأرشفة المراسلات الالكترونية أثناء اللجوء إليها ينتج عنها طمس الدليل الإلكتروني نهائيا لاسيما في حالة عدم التوصل إلى أدلة تقليدية تساعد على نسبة الجريمة إلى المتهم كالإعتراف مثلا، وبهذا تنتفي مسؤوليته الجزائية ، الأمر الذي استلزم وضع إطار قانوني لمعالجة هذه الفوضى ، فإن أحسن سبيل في ذلك هو اتباع نظام إلزام

[1]- رشيدة بوبكر ، المرجع السابق ، ص 445.

مزودي الخدمات بحفظ المعلومات ،وهذا ما أكده المشرع الجزائري بموجب المادة 10 من الفصل الرابع من القانون 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتهما، والتي نصت على أنه " **في إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية** "، وبوضع المعطيات يتعين عليهم حفظها وفقا للمادة 11 أعلاه تحت تصرف السلطات المذكورة[1].

ولذلك سنتناول فيما يلي تحديد مفهوم هذا الإجراء ، وقبل ذلك نوضح المقصود بمزودي الخدمات لاعتبارهم لأنهم هم الحائزون لهذه المعطيات.

الفرع الأول : مفهوم مزودي الخدمات .

يقصد بمزود الخدمات " **من يقدم خدمته إلى الجمهور بوجه عام في مجال الاتصالات الإلكترونية والتي لا تقتصر في أدائها على طائفة معينة من المتعاملين معه بمقتضى عقد من العقود** "[2].

وبالرجوع إلى المشرع الجزائري فقد عرف مقدم الخدمة بموجب نص المادة 2 الفقرة ومن القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتهما بأنه: "

1- **أي كيان عام أو خاص يقدم لمستعملي خدماته ضمانة القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام الاتصالات.**

2- **وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها ".**

ومن خلال نص المادة نستنتج أن المراسلة في البريد الالكتروني تمر على مزود الخدمة للاتصالات الالكترونية قبل أن يتلقاها المرسل إليه تبقى مخزنة داخله إلى حين استقباله لها عن طريق مزود الخدمة ، فبمجرد استلامه لتلك المراسلة تكون قد وصلت إلى وجهتها الأخيرة ، وفي هذه المرحلة يمكن أن يقوم المرسل إليه بمسحها أو تخزينها لدى مزود خدمة الاتصالات الإلكترونية[3].

---

[1]- القانون 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة من الجرائم المتصلة بتكنولوجيا الإعلام ومكافحتهما، الجريدة الرسمية الجزائرية، العدد 47، الصادرة بتاريخ 16 أوت 2009.

[2]- عائشة بن قارة مصطفى ، المرجع السابق ، ص 154.

[3]- رشيدة بوبكر ، المرجع السابق ، ص 447.

الفرع الثاني: مفهوم المعطيات المتعلقة بحركة السير.

يقصد بحفظ المعطيات " **توجيه السلطة المختصة لمزودي الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته أو تحت سيطرته ، في إنتظار اتخاذ إجراءات أخرى كالتفتيش أو الأمر بتقديم بيانات معلوماتية**[1]".

لقد حدد المشرع المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمة المتمثلة في معطيات المرور أو كما سماها " **بحرية السير** "، وقد تم تعريف هذه الأخيرة بموجب نص المادة 2 فقرة ه من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بأنها:" **أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الاتصالات توضح مصدر الاتصال والوجهة المرسل إليها والطريق الذي يسلكه ووقت وتاريخ وحجم مدة الاتصال ونوع الخدمة** ".

ومن خلال هذه الفقرة يتضح أن البيانات المعلوماتية المشمولة بالأمر تتضمن بيانات المرور المتعلقة باتصالات سابقة ، وذلك من أجل تحديد خط سير الاتصال أو مكان وصول هذه الاتصالات،و كذلك زمن الاتصال فهي من الأمور الجوهرية التي تسهل عملية التعرف على هوية الأشخاص المرتكبين لإحدى الجرائم.

وفي أغلب الأحيان يكون مقدم الخدمة هو الوحيد الحائز لبيانات المرور ما يكفي للتحديد بدقة مصدر أو نهاية الاتصال، بل وإن حاز كل واحد منهم على بعض أجزاء اللغز يتعين أن توضع هذه الأجزاء تحت الاختبار قصد تحديد الجهة المرسلة إليها ومصدرها[2].

الفرع الثالث: إلتزامات مزودي الخدمات.

تقع على عاتق مزودي الخدمات مجموعة من الالتزامات نذكر منها :

البند الأول : التزام مزودي الخدمات بمدة معينة للتخلص من المعطيات.

لقد وضع المشرع الجزائري مدة محددة لإزالة المعطيات التي تم تخزينها من طرف مزودي الخدمات احتراما للحق في الخصوصية ، وتقدر هذه المدة بسنة، حيث يبدأ احتسابها من تاريخ التسجيل وهذا بموجب نص المادة 11 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما ،والتي جاء في فحواها : " تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل .. ".

---

[1]- أشرف عبد القادر قنديل ، المرجع السابق ، ص 180.

[2]- عائشة بن قارة مصطفى ، المرجع السابق ، ص 160.

البند الثاني : التزام مزودي الخدمات بعدم التقاعس عن حفظ المعطيات .

لقد فرض المشرع الجزائري مجموعة من الالتزامات على مقدمي الخدمات وهذا بموجب المادة 11 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما، بالإضافة إلى ذلك فهو مقيد بمجموعة من الالتزامات المفروضة عليه في دفتر الشروط، لأن مستعملي هذه الوسائل يتعاملون مع هيئات معينة ولديهم دفتر الشروط يتضمن كل الالتزامات ،وهم ملزمون باحترامها ،فإذا تخلوا عن هذه الالتزامات فتطبق على الإدارة عقوبات إدارية، وإذا قصر أو أهمل أحد مستخدمي هذه الوسائل الالتزامات المذكورة في دفتر الشروط بعد تطبيق العقوبات الإدارية عليه ، تقوم بمتابعته جزائيا لأنه في هذه الحالة يعرقل السير العادي للعدالة[1].

خاتمة

للإثبات أهمية بالغة من الناحية العلمية فهو يفيد في تحديد مكان وزمان إرتكاب الجريمة والأداة المستخدمة فيها، بالإضافة إلى تحديد الجاني أو الجناة في حالة التعدد ، كما أنه يساعد على بيان درجة خطورتهم ويوضح كذلك الأسلوب الإجرامي المتبع لتنفيذ جريمتهم، بالإضافة إلى ذلك فإن الإثبات يساهم في مساعدة المحكمة على تصور كيفية وقوع النشاط الإجرامي وبيان المراحل السابقة لإرتكاب الجريمة ،وتحديد جميع ملابساتها وذلك من خلال اطلاعها على الأدلة المادية والقرائن، وما أدلى به الشهود والمتهمين من أقوال واعترافات تخرج المحكمة من نطاق الشك إلى اليقين .

ويعد الإثبات الجنائي العمود الفقري للنظام القضائي، فهو الأساس الذي يقوم عليه القضاء، حيث أنه الملجأ الوحيد للقاضي في حل نزاعات الأفراد، ورغم المؤهلات التي يتمتع بها، إلا أنه يبقى بشرا يستحيل عليه الإحاطة بجميع الحوادث والإلمام بجميع الوقائع بنفسه ، فهو أمام خصمين يدعى كل منهما الحق لنفسه ، مما يحتم عليه اللجوء إليه ، وذلك من أجل تحقيق العدل والإنصاف بين أفراد المجتمع.

وبعد التعرض لأدلة الإثبات الجنائية الحديثة وطرق البحث والتحري في الجريمة المعلوماتية الحديثة ، توصلنا إلى نتيجة وهي أن هذه الصعوبات المتعلقة بالدليل ذاته، وهي أن الصعوبات ناتجة عن كون القواعد التقليدية قاصرة في الكشف عن الأدلة ،لذلك لابد من وجود قواعد

[1]- رشيدة بوبكر ، المرجع السابق ، ص 452.

خاصة تراعى طبيعة الدليل ، وتقرر إجراءات خاصة يجب إتباعها ، وقد تمت معالجو ذلك خلال البحث ، وتم التوصل إلى التوصيات التالية:.

- إن حجية الأدلة الجنائية في مجال الإثبات الجنائي مقيدة بجموعة من الشروط المتعلقة بإجراءات التحقيق المخصصة لاستخلاص الأدلة الالكترونية بحيث يفرض على السلطات المختصة بأن تقوم بالحصول عليها بطريقة مشروعة.
- الحرص على تدريب رجال البحث والتحري والخبراء والقضاة على التعامل مع الجرائم الالكترونية من الناحيتين الفنية والعملية.
- العمل على تكريس قواعد قانونية جديدة تتناسب مع طبيعة الجرائم المعلوماتية.
- تطوير ثقافة الحاسب الآلي وسط رجال الأمن، وذلك من حيث القدرة على الملاحظة ومراعاة تصرفات الأشخاص العاملين في مجال الحاسب الآلي بدقة ، أو المهتمين بالبرمجة أو هواة صناعة الأنظمة المعلوماتية وتقليدها ، فدراسة تصرفات هؤلاء ورقابتها تعد مدخلا جيدا للسيطرة الأمنية عليهم وضبطهم.

ضوابط تحديد الاختصاص الجزائي في الجرائم المعلوماتية

Controls for determining criminal jurisdiction in information crimes

د.صحراوي نور الدين
جامعة أبو بكر بلقايد تلمسان – الجزائر

مقدمة:

ترتب على ظاهرة الجريمة االمعلوماتية تحديات عديدة منها ظهور وتنامي الأنشطة الإجرامية الالكترونية وتميز مرتكبيها بتقنيات جديدة غير مسبوقة في مجال تكنولوجيا المعلومات والاتصالات يسرت لهم ارتكاب هذه الأنشطة داخل حدود الدولة وخارجها الأمر الذي أدى إلى انشغال المنظمات والمؤتمرات الدولية بهذا النوع من الجرائم ودعوتها الدول إلى التصدي لها ومكافحتها ، من حيث تستعصي بعض الأنشطة على إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية ؛ ومن حيث ما يرتبط بهشاشة نظام الملاحقة الإجرائية التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة ، سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجنائية الدولية .

وعلى صعيد الملاحقة الإجرائية من ناحية أخرى ، فإن هذا أمر يستلزم، أولا الانطلاق من الاقتناع بخطورة هذه الظاهرة ، ومحاولة التوفيق بين احترام مبدأ السيادة الوطنية لكل دولة في صورته التقليدية ، والنزول ولو بقدر أمام ضرورات ومقتضيات التعاون القضائي الدولي الذي بقدر نجاحه تحقق فعالية كل الجهود والإمكانيات المسخرة للتصدي لظاهرة الجرائم الإلكترونية ومكافحتها، فهنا يطرح مشكل الإختصاص القضائي في الجريمة الإلكترونية و ذلك في ظل غياب إطار تشريعي يحكمه و ينظمه يتم التعامل معه وفق قواعد الإختصاص المحلي و هذا ما يطرح جملة من الصعوبات ، خصوصا أن مكان ارتكاب الجريمة الإلكترونية و الذي يكون دائما في البيئة الافتراضية غير الملموسة يختلف عن مكان ارتكاب باقي الجرائم التقليدية الأخرى في العالم المادي الملموس.

إن المقصود بالاختصاص القضائي هو السلطة السيادية للدولة التي تمكنها من تطبيق قوانينها الوطنية داخل إقليمها، و تعد الجرائم المعلوماتية من أكثر الجرائم التي تطرح إشكالية الاختصاص القضائي و ذلك على أساس أن السلوك الإجرامي فيها ليس له حدود معينة، بل الأكثر من ذلك

فان العالم كله مرهون بمجرد نقرة بسيطة على لوحة المفاتيح لجهاز الحاسوب أو الهواتف النقالة الذكية.

و إن الطبيعة التقنية العالية لنظم المعلوماتية المرتبطة بشبكات الاتصال العالمية يمكن أن تؤدي إلى أن يصبح إقليم أكثر من دولة مسرحا للجريمة المعلوماتية الأمر الذي قد يجر عنه السقوط في مشكلة تنازع الاختصاص بين هذه الدول، مثلا يمكن أن ترتكب هذه الجريمة في إقليم الدولة الجزائرية و تحقق النتيجة الجرمية في إقليم الدولة الفرنسية، ومن ثم تتعدد القوانين التي يمكن أن تحكم هذه الجريمة بتعدد الدول المرتبطة بها.

و تبرز أهمية هذا الموضوع في أن الجريمة المعلوماتية تعد عالمية أي أنها لا تحكمها حدود جغرافية معينة، حيث أنه يمكن ارتكاب الفعل الإجرامي في مكان معين و تحقق النتيجة في مكان آخر وقد يكون الضحية في مكان ثالث، بل و قد تكون هذه الأماكن في دول مختلفة، ولذلك ارتئينا تسليط الضوء على تطبيق القاعدة الجزائية من حيث المكان على هذا النوع المستحدث من الجرائم.

و تهدف هذه المداخلة الى تحقيق هدف رئيسي متمثل في محاولة تقديم دراسة تبين المبادئ التي تحكم تطبيق القانون من حيث المكان و مدى ملائمتها مع هذا النوع المستحدث من الجرائم، و هذا ما أدى بنا إلى طرح الإشكالية التالية، ما هو القانون الواجب التطبيق على هذا النوع من الجرائم المستحدثة، و ماهي المحكمة المختصة إقليميا بالنظر في الدعوى؟.

للإجابة على هذه الإشكالية ارتأينا تقسيم هذه المداخلة إلى مبحثين، تعرضنا في المبحث الأول إلى القانون الواجب التطبيق على الجرائم المعلوماتية، و في المبحث الثاني تطرقنا إلى الاختصاص المحلي في هذا النوع من الجرائم.

ونظرا لطبيعة الموضوع و غايته المتمثلة في تحديد الاختصاص القضائي من حيث المكان و القانون الواجب التطبيق، سيتم استعمال المنهج التحليلي و ذلك بذكر المبادئ العامة التي تحكم تطبيق القانون من حيث المكان.

المبحث الأول: القانون الواجب التطبيق على الجريمة المعلوماتية

نظرا لحداثة هذا النوع من الجرائم المرتكبة عبر الوسائط الالكترونية، فإنها حظيت بكثير من الاهتمام و التعاون في المجتمع الدولي ومن أهم هذه الجهود ما عمد إليه مجلس وزراء العدل للدول العربية في دورته التاسعة عشر[1]، و كذا مجلس وزراء الداخلية للدول العربية في دورته

[1] - المنعقد بتاريخ 2003/10/08 بالقرار رقم 495.

الواحد و العشرين[1] وذلك بتبني القانون العربي النموذجي لمكافحة جرائم الكمبيوتر و الانترنيت، بحيث نص هذا القانون في مادته 22 على أنه " تسري أحكام التشريع الجنائي للدولة على الجريمة المعلوماتية إذا ارتكبت كلها أو جزء منها داخل حدودها وفقا لمبدأ الإقليمية، كما تختص المحاكم فيها بنظر في الدعاوى الناشئة على هذه الجرائم، و على الدول العربية عقد اتفاقيات لتبني المعيار الأول في حالة تنازع الاختصاص بين الدول"[2].

و عليه فان القانون الجنائي للدولة يسري على الجريمة المعلوماتية التي تقع خارج حدودها إذا كانت تمس بأمنها وفقا للقواعد العامة المنصوص عليها في قانون العقوبات[3]، و هذا ما نص عليه المشرع الجزائري بحيث تسري أحكام قانون العقوبات الجزائري داخل إقليم الجمهورية الجزائرية على كل شخص ارتكب جريمة في نظر القانون الجزائري سواء أكان مواطنا جزائريا أو أجنبيا[4].

و من خلال ما سبق و لتبيان القانون الواجب التطبيق على الجريمة المعلوماتية، لا بد من التمييز بين الجرائم المرتكبة داخل الإقليم الوطني (المطلب الأول)، و الجرائم المرتكبة خارج الإقليم الوطني (المطلب الثاني).

المطلب الأول: الجريمة المعلوماتية المرتكبة داخل الإقليم الوطني

يتحدد الإقليم الوطني بالمساحة الأرضية التي تباشر الدولة عليها سيادتها و تنظم و تقوم فيها بالخدمات العمومية و هو ما يعرف بالإقليم البري، زائد الإقليم البحري، بالإضافة إلى الفضاء الذي يعلو الإقليم البري و الإقليم البحري كما تمتد سيادة الدولة إلى السفن و الطائرات التي تحمل علمها، و السفن و الطائرات الأجنبية إذا هبطت أو رست في المطارات أو الموانئ الجزائرية[5].

و قد كرس المشرع الجزائري على غرار أغلب التشريعات العالمية مبدأ الإقليمية للنص الجنائي، و الذي مفاده تطبيق القانون الوطني للدولة على كل جريمة ارتكبت داخل إقليمها مهما كانت

---

[1] - المنعقد في 21 أبريل 2004.

[2] - أنظر، بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي و الداخلي، أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر 01، السنة الجامعية 2017- 2018، ص 197.

[3] - المادة 03 من ق.ع.ج.

[4] - أنظر، علي عبد الله سليمان، شرح قانون العقوبات الجزائري، القسم العام، الجزء الأول (الجريمة)، ديوان المطبوعات الجامعية، الجزائر، ص 115.

[5] - المادة 12 من الدستور الجزائري.

جنسية مرتكبيها[1]. و تعتبر الجريمة مرتكبة في الجزائر كل جريمة يكون أحد الأعمال المميزة لأركانها تم في الجزائر[2].

أما عن موقف المشرع الفرنسي، فان القضاء الفرنسي نادى إلى التوسيع في تحديد مكان وقوع الجريمة الذي من مظاهره تدويل فكرة مكان وقوع الجريمة من حيث الواقع ، واعتبار كل دولة مختصة بنظر هذه الجريمة ، ويمكن رصد مظاهر ذلك التوسع في مجال الجرائم الوقتية متعدية الآثار، فعلى الرغم من تنفيذ الجريمة على إقليم دولة إلا أن آثار هذه الجريمة قد تتعدى حدود دولة التنفيذ ، ولم يتنكر القضاء الفرنسي لانعقاد اختصاصه بنظر مثل هذه الجريمة لكون آثارها قد تحققت على الإقليم الفرنسي ، كما في إحدى جرائم النشر التي وقعت بواسطة صحيفة تم طبعها وتوزيعها في دولة أجنبية ، لكن بعضا من نسخها قد وزع في فرنسا[3] ، كما أجاز القانون والقضاء الفرنسيين بنظر جريمة اعتداء على الملكية الفكرية وقعت في الخارج متى كانت آثارها قد تحققت في فرنسا[4].

وإعمال السريان المكاني للقانون الجنائي وفقا لمبدأ الإقليمية ، لا يخلو من صعوبات، تفضي تارة إلى إثارة تنازع إيجابي في الاختصاص بين أكثر من تشريع وطني ، وتارة أخرى يقوم تنازع سلبي في الاختصاص يخرج معه اختصاص أي من الدول بملاحقة الجاني ، وهذا النوع الأخير من التنازع نادر الوقوع لأن التشريعات الوطنية تعقد اختصاصها وفقا لمعايير الاختصاص المعروفة.

أما في حالة قيام تنازع إيجابي في الاختصاص بين أكثر من دولة لملاحقة نفس النشاط الإجرامي، أو في حالة يثور فيها التنازع كما في الجرائم العابرة للحدود التي يتوزع فيها السلوك المادي للجريمة في إقليم أكثر من دولة ، أوفي حالة تجرد بعض عناصر هذا السلوك من خصوصيتها المادية، كما هو الحال في المساهمة الجنائية التي تتم باستخدام أجهزة الاتصالات الحديثة ؛ مثل هذه الظاهرة تفرض تنازعا في الاختصاص بل غموضا في تحديد معياره ، تتطلب بطبيعة الحال

---

[1] - المادة 03 من الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون العقوبات، المعدل والمتمم.

[2] - المادة 58 الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون الإجراءات الجزائية، المعدل و المتمم بالقانون رقم 04-14 المؤرخ في 10 نوفمبر سنة 2004 ، ج.ر. 10 نوفمبر 2004، عدد 71، ص. 04.

[3]- Cass. Crim. 30 avril1908 1,p.553,note.

[4] - Cass. Crim. 2 fevrier 1977,d.1977, information rapide,137, paris30 mars 1987 . C.P.,1988,11,n20965,obs.p.Bouzat.

حلولا مستحدثة وابتكارا لمفاهيم قانونية جديدة دون إخلال بمبادئ الشرعية الجنائية التي ترتكز عليها معظم النظم الجنائية الوطنية[1] .

المطلب الثاني: الجرائم المرتكبة خارج الإقليم الوطني

بما أنه و تطبيقا لمبدأ الإقليمية فان القانون الوطني القانون الوطني للدولة على كل جريمة ارتكبت داخل إقليمها مهما كانت جنسية مرتكبيها، إلا أنه ترد بعض الاستثناءات على هذا المبدأ، وذلك أنه يمكن أن يطبق القانون الوطني على الجرائم المرتكبة خارج الإقليم الوطني في حالات استثنائية حددها المشرع[2].

إذ يطبق القانون الجزائري على الجرائم بما فيها المعلوماتية إذا كان مرتكبها جزائري حتى و لو تم ارتكابها خارج الإقليم الجزائري[3] لكن يشترط لتطبيق القانون الجزائري في هذه الحالة، أن يكون الجاني جزائريا وقت ارتكاب الجريمة، و أن يكون الفعل مجرما في كلا التشريعين و له وصف جناية أو جنة، كما يشترط ألا يكون قد صدر في حق الجاني حكم نهائي من طرف محكمة أجنبية و لنفس الوقائع إذ لا يجوز متابعة شخص مرتين على نفس الأفعال، و أخيرا يشترط عودة المتهم إلى الجزائر[4].

وكذلك يطبق القانون الجزائري على الجرائم الماسة بأمن و سلامة الدولة الجزائرية بغض النظر عن جنسية مرتكبها و مكان ارتكابها، و هذا تكريسا لمبدأ الدفاع عن السيادة الوطنية[5]. بحيث يجوز متابعة كل أجنبي وفقا لأحكام القانون الجزائري إذا القي عليه القبض في الجزائر أو حصلت الحكومة تسليمه لها، ارتكب خارج الإقليم الجزائري بصفة فاعل أصلي أو شريك في جناية أو

[1] - التنازع السلبي في الاختصاص يتعين تقرير مبدأ الاختصاص العالمي الذي يعطي لدولة القبض على المتهم الاختصاص بملاحقته إذ كان يحمل جنسيتها ، فإن لم يمكن كذلك ، وجب تسليمه في حالة المطالبة به من دولة أخرى وفقا لمبدأ الإقليمية أو الشخصية

[2] - المواد من 582 إلى 588 من ق.ا.ج.ج.

[3] - المواد 582 و 583 من ق.ا.ج.ج.

[4] - أنظر، أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، الجرائم ضد الأشخاص و الجرائم ضد الأموال، الطبعة الخامسة، دار هومه، 2006، ص 91.

[5] - أنظر، سعيداني نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، كلية الحقوق، جامعة باتنة، السنة الجامعية 2012- 2013، ص 98.

جنحة ضد سلامة الدولة الجزائرية أو تزييف النقود أو أوراق مصرفية وطنية متداولة قانونا بالجزائر[1].

وقد يثور جدل في مسألة تخزين المعلومات أو البيانات المعالجة إلكترونياً خارج إقليم الدولة، وعلى هذا الأساس انقسم الفقه في موقفه لتقدير هذه المسالة، فذهب البعض إلى أنه من غير المشروع أن تقوم سلطات دولة ما بالتدخل وتفتيش النظم المعلوماتية الموجودة في إقليم دولة أخرى ، بهدف كشف وضبط أدلة لإثبات جريمة كانت قد وقعت على أراضيها وذلك استنادا إلى مبدأ إقليمية القانون، وبهذا الرأي قضت إحدى المحاكم الألمانية في جريمة غش ارتكبت في ألمانيا بأن الحصول على البيانات الخاصة بهذه الجريمة والمخزنة بشبكات اتصال موجودة في سويسرا لا يتحقق إلا بطلب المساعدة من الحكومة السويسرية وفي واقعة نشر فيروسLove bug عام 2000 الذي تسبب في إتلاف المعلومات في أجهزة الحاسب الآلي، فعندما اكتشف الخبراء الأمريكيون بأن هذا الفيروس أرسل من الفليبين فان تفتيش منزل المشتبه فيه تقتضي تعاون السلطات الفليبينية والحصول على إذن من قاضي التحقيق بالفليبين[2].

أما الرأي الثاني ، فإنه يعتمد على أن القانون الدولي يمكن أن يتشكل من خلال توافق الآراء على الصعيد الدولي باتجاه السماح بتنفيذ هذه الإجرأءات حال توافر ظروف معينة يتم تحديدها، كإشعار الدولة المراد تفتيش البيانات والمعلومات المخزنة بنظمها المعلوماتية وعلى هذه الكيفية أصدر المجلس الأوروبي في 11 سبتمبر 1995 توصية من بين عدة توصيات تناولت مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات ، جاء فيها بأن تفترض إجراءات التحقيق مد الإجراءات إلى أنظمة حاسب آلي أخر قد تكون موجودة خارج الدولة وتفترض التدخل السريع، وحتى لا يمثل مثل هذا الأمر اعتداء على سيادة الدولة أو القانون الدولي ، وجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الإجراء ، ولذلك كانت الحاجة ملحة لإبرام اتفاقيات تنظم وقت وكيفية اتخاذ مثل هذه الإجراءات كما يجب أن تكون هناك إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة ، ويتعين عندئذ أن تسمح السلطة الأخيرة بإجراءات التفتيش والضبط ، ويتعين كذلك

[1] - المادة 588 من ق.ا.ج.ج.

[2] - أنظر، هشام محمد فريد رستم ، الجوانب الإجرامية للجرائم المعلوماتية ، مكتبة الآلات الحديثة ، 1994، ص 71، وأنظر كذلك، اهلالى عبدا لاه احمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتى ، دار الحديث للنشر ، 2009 ، ص77 .

السماح لهذه السلطة بإجراء تسجيلات للتعاملات الجارية وتحديد مصدرها، وهذا كله لا يتأتى إلا بتفعيل اتفاقيات التعاون الدولي وتكريسها [1].

والتساؤل الذي يثور هو كيف يمكن إعمال مبدأ الإقليمية على الجرائم التي ترتكب بواسطة شبكة المعلومات الدولية الإنترنت، وكيف يمكن أيضا تحديد إقليم الدولة الذي وقعت عليه مثل هذه الجرائم بتعددها وتنوعها وتعقيدها ؟ الإجابة هي أن التقدم العلمي الراهن وتطور وسائل الاتصال الحديثة كالإنترنت وسائر صور الاتصال الإلكتروني عبر الأقمار الصناعية ، أتاح فرصا هائلة للخروج على مبدأ الإقليمية ، وتبني مدونة جديدة لفض مثل هذا التنازع أو بالأقل ترتيب معاييره ، لأن معيار إقليمية القانون لم يعد هو المعيار الوحيد ، ولا ربما الأكثر قبولا في بعض الجرائم ، بل ازدادت أهمية معايير أخرى كانت فيما مضى تعد احتياطية كمعيار العينية ومعيار العالمية ؛ وظهرت الأهمية البالغة لمبدأ المحاكمة أو التسليم ولو في صورته المعكوسة : التسليم أو المحاكمة[2].

المبحث الثاني: الاختصاص المحلي في الجرائم المعلوماتية

يقصد بالاختصاص المحلي أو كما يطلق عليه البعض الاختصاص الإقليمي باعتبار أن القضاء الوطني هو المختص بالنظر في الدعاوى الجنائية، و يقوم هذا الاختصاص على تحديد دائرة الاختصاص المكاني و الجغرافي لمنطقة معينة من إقليم الدولة[3].

و ينعقد الاختصاص المحلي للمحاكم بناء على ثلاثة معايير[4]، فان الاختصاص المحلي لوكيل الجمهورية و قاضي التحقيق يتحدد أولا بمكان وقوع الجريمة، ثانيا يتحدد بمحل إقامة أحد الأشخاص المشتبه

---

[1] - أنظر، عمر عبيد محمد الغول، جرائم الكمبيوتر، دار الثقافة للطبع و النشر، القاهرة، 1999 ، ص 204.

[2] - يمثل تسليم المجرمين مظهرا من مظاهر التعاون الدولي في مكافحة ظاهرة الإجرام ، فتقوم دولة من الدول بمطالبة دولة أخرى بتسليمها شخصا ينسب إليه ارتكاب جريمة أو صدر حكم بالعقوبة ضده حتى تتمكن الدولة الطالبة - باعتبارها صاحبة الاختصاص - من محاكمته أو من تنفيذ العقوبة الصادرة في حقه . ويستمد النظام القانوني لتسليم المجرمين مصدره أحيانا من أحكام التشريع الوطني ، ولكن الغالب يكون مصدره الاتفاقيات الدولية أو شبه الدولية أو الثنائية ، وقد يستند التسليم إلى قواعد العرف الدولي أو اتفاق المعاملة بالمثل . والتسليم أكثر جدوى لإدارة إستراتيجية مكافحة الجرائم الإلكترونية ، ولا تتأكد فعاليته إلا بتحقق أمرين أولهما، تجاوز اعتبارات السيادة القضائية ولو بقدر ضرورات التعاون الدولي ؛ ثانيهما قيام التشريعات الوطنية بتفعيل هذا التعاون وتنظيمه وفق ما تقتضيه المعاهدات الدولية ذات الصلة .

[3] - أنظر، بدري فيصل، المرجع السابق، ص 200.

[4] - المواد 37 و 40 من ق.ا.ج.ج.

في مساهمتهم في ارتكاب الجريمة، و ثالثا يتحدد بمحل القبض على أحد المشتبه فيهم و لو تم القبض لسبب آخر[1].

و عليه سوف نتعرض في هذا المبحث إلى المبدأ العام في تحديد الاختصاص المحلي (المطلب الأول)، ثم نتعرض إلى إجراءات تمديد الاختصاص المحلي (المطلب الثاني).

المطلب الأول: المبدأ العام في تحديد الاختصاص المحلي للجريمة المعلوماتية

وفقا لهذا المبدأ فان المحكمة التي تختص للنظر في الدعاوى الجنائية هي المحكمة التي ارتكبت في دائرة اختصاصها الجريمة المعلوماتية. ويتحدد مكان وقوع الجريمة حسب نوعها، فالجريمة التي ترتكب دفعة واحدة و في زمن واحد يعتبر مكان وقوعها هو نفسه مكان تنفيذ الفعل الإجرامي، أما الجريمة التي تتطلب لارتكابها عدة أفعال و في أماكن مختلفة فان الاختصاص المحلي ينعقد لكل محكمة وقع في دائرة اختصاصها فعل من الأفعال المنفذة وفقا لهذا المعيار، أما إذا تعلق الأمر بجريمة مستمرة فان كل مكان تقوم فيه حالة الاستمرار يعتبر مكان لوقوع الجريمة[2].

كما يكون لمحكمة إقامة المشتبه فيه الاختصاص، فان كل محكمة يقع في اختصاصها محل إقامة المشبه فيهم مساهمتهم في ارتكاب الجريمة تكون مختصة إقليميا بالنظر في الدعوى الجنائية، و العبرة في هذه الحالة بمحل الإقامة و الذي يتحدد وقت ارتكاب الجريمة.

كما تكون المحكمة مختصة إقليميا إذا تم في دائرة اختصاصها القبض على أحد المشتبه فيهم فتكون لها ولاية النظر في الجريمة المعلوماتية، حتى لو كان القبض على المشتبه فيه غير الجريمة محل المتابعة، أما بالنسبة للجرائم التي يرتكبها الأحداث[3] فان الاختصاص المحلي ينعقد للمحكمة التي ارتكبت الجريمة في دائرة اختصاصها، أو محل إقامة الحدث أو والديه أو وصيه أو محكمة المكان الذي عثر فيه على الحدث أو المكان الذي أودع فيه الحدث سواء بصفة مؤقتة أو نهائية[4].

وباختصار فإنه يتحدد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، فإذا وقعت جريمة ما في دائرة اختصاص محكمة معينة (دائرة قضائية) فإن وكيل الجمهورية لدى المحكمة المختصة محليا هو المختص بالإجراءات الجزائية الواجب اتخاذها إزاء الجريمة المرتكبة هذا إذا ألقي القبض

---

[1] - أنظر، جيلا لي بغدادي، التحقيق، الديوان الوطني للأشغال التربوية، الطبعة الأولى، 1999، ص 108.

[2] - أنظر، بدري فيصل، المرجع السابق، ص 201.

[3] - المادة 451 من ق. اج.ج.

[4] - أنظر، عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، التحري و التحقيق، دار هومه، 2008، ص 324.

على المجرم الذي قام باقتراف هذه الجريمة. أما إذا لم يقبض على المجرم، بل فر هاربا فإن وكيل الجمهورية المختصة هو الذي يقع بدائرته مقر إقامة المجرم المتهم أو أحد الأشخاص المشتبه في مساهمتهم فيها، إذا كان له محل إقامة معين، أما إذا قبض على المتهم أو المشتبه فيه فإن وكيل الجمهورية المختص هو الذي تم في دائرته القضائية مقر إقامة المجرم المتهم أو أحد الأشخاص المشتبه في مساهمتهم فيها، إذا كان له محل إقامة معين، أما إذا قبض على المتهم أو المشتبه فيه فإن وكيل الجمهورية المختص هو الذي تم في دائرته القضائية القبض على المتهم[1].

كما يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة، أو بمحل إقامة احد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى و لو كان القبض قد حصل لسبب أخر[2].

كما يمكان يمتد اختصاص قاضي التحقيق إلى كامل التراب الوطني في حالات خاصة لضرورة التحقيق في الجرائم معينة ومن بينها الجرائم المعلوماتية ، يمكن لقاضي التحقيق أن يقوم بأي عملية تفتيش أو حجز ليلا أو نهارا و في أي مكان على امتداد التراب الوطني أو بأمر ضابط الشرطة القضائية المختصين بذلك[3].

ومنه فإن الإختصاص الإقليمي حدد في المادة 40 قاإج و يتحدد الإختصاص المحلي إما بمكان وقوع الجريمة و إما بمحل إقامة المتهم و إما بمكان الذي تم فيه القبض على المتهم حتى و لو كان القبض لسبب آخر. و يمكن ان يمتد اختصاصه الى دائرة اختصاص المجلس القضائي ذلك في الجرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بموجب التعديل نوفمبر 2004 [4].

كما تجدر الإشارة إلي أن الإختصاص الشخصي لقاضي التحقيق يحقق في كل الجرائم سواء كانت جنايات أو الجنح و المخالفات التي قدمت بشأنها النيابة العامة طلبا افتتاحيا، كما يحقق مع الأشخاص الذين لم توجه لهم التهمة بارتكابهم نفس الوقائع و الذين لم يرد اسمهم في الطلب الإفتتاحي[5].

---

[1] - المادة 37 من ق. اج.ج.

[2] - المادة 40 من ق. اج.ج.

[3] - المادة 47 من ق. اج.ج.

[4] - المادة 40 الفقرة 02 من ق. اج.ج.

[5] - المادة 67 الفقرة 03 من ق. اج.ج.

وعليه فان الاختصاص المحلي في الجريمة المعلوماتية وفق هذه المعايير قد ينعقد لعدة محاكم في نفس الجريمة، فالمحكمة التي كان لها السبق في إجراءات المتابعة هي المختصة إقليميا[1].

المطلب الثاني: تمديد الاختصاص المحلي في الجرائم المعلوماتية

الأصل أن الاختصاص الإقليمي في القضاء الجزائي يتحدد استنادا إلى المعايير معينة... لكن ثمة حالات وضروريات قانونية وعملية استلزمت أن يخرج فيها المشرع عن القواعد العامة في الاختصاص، وذلك بتقرير امتداد اختصاص إحدى المحاكم الجزائية لتصبح مختصة بالنظر في قضايا لم تكن أصلا من اختصاصها[2].

وكما سبق الذكر فان الاختصاص المحلي قد ينعقد لعدة محاكم في نفس الجريمة خاصة في الجريمة المعلوماتية لكن النظر فيها يكون من اختصاص محكمة واحدة، و قد تؤدي الضرورة الملحة للتحري و الاستدلال و التحقيق بمخالفة دائرة الاختصاص و القيام بإجراءات التفتيش والتسرب و المراقبة و غيرها بان تكون في دوائر اختصاص محاكم أخرى، على هذا الأساس سمح المشرع الجزائري بتمديد الاختصاص في قانون الإجراءات الجزائية الجزائري[3].

كما يجوز لقاضي التحقيق الانتقال إلى دوائر اختصاص المحاكم المجاورة للدائرة التي يقوم فيها بوظيفته للقيام بكل الإجراءات التي يقتضيها السير الحسن للتحقيق في الجرائم المعلوماتية إذا استلزمت ضرورات التحقيق فيها ذلك بشرط إخطار وكيل الجمهورية المختص إقليميا و تعداد الأسباب التي أدت إلى انتقاله[4].

كما أجاز المشرع الجزائري تمديد الاختصاص المحلي لوكيل الجمهورية و قاضي التحقيق عن طريق التنظيم إلى دائرة اختصاص محاكم أخرى في بعض الجرائم و من بينها الجرائم المعلوماتية[5]، و قد المشرع إلى أبعد من هذا بحيث منح لقاضي التحقيق إمكانية القيام بإجراءات الحجز و التفتيش في أي ساعة من الليل أو النهار و في أي مكان على امتداد التراب الوطني إذا تعلق الأمر بجريمة

---

[1] - أنظر، أحسن بوسقيعة، المرجع السابق، ص 93.

[2] - محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري ، دار هومة ، الطبعة الثالثة، الجزائر، 2008، ص 21.

[3] - المادة 329 من ق. اج.ج.

[4] - المادة 80 من ق. اج.ج.

[5] - المواد 37 و 40 من ق.اج.ج.

معلوماتية[1]، سواء قام بذلك بنفسه أو بموجب إنابة قضائية لضباط الشرطة القضائية المختصين إقليميا[2].

وعليه فان إجازة المشرع لتمديد الاختصاص المحلي فيه تخطي لمشكلة عويصة قد تتسبب في عرقلة إجراءات التحقيق و تؤدي إلى إثارة ما يسمى بتجاوز الاختصاص، خاصة أن قواعد الاختصاص المحلي تعد من النظام العام و يمكن إثارتها في أية مرحلة كانت فيها الدعوى كما يمكن للمحكمة إثارة هذا الدفع من تلقاء نفسها[3].

وفي هدا السياق، نص المشرع الجزائري صراحة على امتداد الاختصاص المحلي لبعض المحاكم، بالنظر في بعض الجرائم التي تدخل في الأصل في الاختصاص الإقليمي لمحاكم أخرى، ومن بين هذه الجرائم نجد الجريمة المنظمة العابرة للحدود وجرائم أخرى تشكل صورة من صور هذه الجريمة، مثل الجرائم المعلوماتية[4].

واستجابتا للتعديل الحاصل في قانون الإجراءات الجزائية الجزائري سنة 2004 ، المتعلق بتمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، جاء المرسوم التنفيذي رقم 06- 348[5]، ليحدد المحاكم المعنية بالتمديد والنطاق المكاني الذي أضحى يدخل ضمن اختصاصها، إذا تعلق الأمر ببعض الجرائم التي على أسسها تم التمديد.ومن خلال استقراء أحكام المرسوم التنفيذي المذكور أعلاه، يتضح بأن تمديد الاختصاص المحلي لبعض المحاكم يكون على النحو التالي:

- محكمة سيدي أمحمد، يمتد الاختصاص المحلي لمحكمة سيدي أمحمد ليشمل محاكم المجالس القضائية للجزائر، الشلف، الأغواط، البليدة، البويرة، تيزي وزو، الجلفة، المدية، المسيلة، بومرداس تيبازة وعين الدفلى[6] .

---

[1] - المادة 47 من ق.ا.ج.ج.

[2] - أنظر، جيلا لي بغدادي، المرجع السابق، ص 111.

[3] - أنظر، بدري فيصل، المرجع السابق، ص 202.

[4] - المادة 40 مكرر من ق.إ.ج.

[5] - مرسوم تنفيذي رقم 06 - 348 مؤرخ في 12 رمضان 1427 الموافق 5 أكتوبر 2006 ، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج. ر.ج ج. ع 63 بتاريخ 8 أكتوبر 2006.

[6] - المادة 2 من المرسوم نفسه.

-محكمة قسنطينة، يمتد الاختصاص المحلي لمحكمة قسنطينة ليشمل اختصاص محاكم المجالس القضائية لقسنطينة، أم البواقي، باتنة، بجاية، بسكرة، تبسة، جيجل، سطيف، سكيكدة، عنابة قالمة، برج بوعريرج، الطارف، الوادي، خنشلة، سوق أهراس وميلة[1] .

-محكمة ورقلة، يمتد الاختصاص المحلي لمحكمة قسنطينة ليشمل اختصاص محاكم المجالس القضائية لورقلة، أدرار، تمنراست، إليزي، تندوف وغرداية[2] .

-محكمة وهران، يمتد الاختصاص المحلي لمحكمة وهران ليشمل اختصاص محاكم المجالس القضائية لوهران، بشار، تلمسان، تيارت، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض تيسمسيلت، النعامة، عين تموشنت وغليزان[3] .

ما تجب الإشارة إليه أن رئيس المجلس القضائي الذي تقع في دائرة اختصاصه المحكمة التي تم تمديد اختصاصها، يختص بالفصل بموجب أمر لا يقبل لأي طعن في الإشكالات التي قد يثيرها تطبيق أحكام التمديد[4] .

وقصد تنسيق العمل بين مختلف الجهات القضائية ولضمان عدم التنازع بين المحكمة المختصة أصالة، استنادا إلى القواعد العامة، والمحكمة التي أصبحت مختصة نتيجة تمديد اختصاصها المحلي، اشترط المشرع الجزائري ضرورة مراعاة أحكام معينة، تتجلى

فيما يلي:

-قيام ضباط الشرطة القضائية بالإخبار الفوري لوكيل الجمهورية لدى المحكمة الكائن بها مكان الجريمة، ويبلغونه بأصل ونسختين من إجراءات التحقيق، فيقوم هو بدوره بإرسال النسخة الثانية إلى النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة[5] .

-يطالب النائب العام فورا باتخاذ الإجراءات، وفي هذه الحالة يتلقى ضباط الشرطة القضائية العاملون بدائرة اختصاص المحكمة الممدد اختصاصها، التعليمات مباشرة من وكيل الجمهورية لدى هذه المحكمة[6] .

---

[1] - المادة 3 من المرسوم نفسه.

[2] - المادة 4 من المرسوم نفسه.

[3] - المادة 5 من المرسوم نفسه.

[4] - المادة 6 من المرسوم نفسه.

[5] - المادة 40 مكرر 1 من ق.إ.ج.

[6] - المادة 40 مكرر 2 من القانون نفسه.

-طلب النائب العام لمباشرة الإجراءات يجوز أن يكون في جميع مراحل الدعوى، وإذا تم فتح تحقيق قضائي، فإن قاضي التحقيق التابع للمحكمة المختصة في الأصل يصدر أمرا بالتخلي عن الإجراءات لفائدة قاضي التحقيق لدى المحكمة التي أصبحت مختصة نتيجة لتمديد اختصاصها، ويكون لهذا الأخير الحق في توجيه تعليمات مباشرة إلى ضباط الشرطة القضائية العاملون بدائرة اختصاص هذه المحكمة الأخيرة[1]. مع إمكانية الأمر باتخاذ كل إجراء تحفظي أو تدبير أمن زيادة على حجز الأموال المتحصل عليها من الجريمة أو التي استعملت في ارتكابها، سواء من تلقاء نفسه أو بناء على طلب من النيابة العامة[2] .

-إذا كان قد صدر أمر بالقبض أو الأمر بالحبس المؤقت ضد المتهم، فإن هذا الأمر يحتفظ بقوته التنفيذية إلى أن تفصل فيه المحكمة التي أصبحت مختصة نتيجة تمديد اختصاصها[3] .

كما أن المشرع الجزائري تفطن إلى مشكلة أخرى مرتبطة بالجريمة المعلوماتية ألا و هي مشكلة ترابط الأنظمة المعلوماتية ببعضها البعض و التي تؤثر في سرعة و نجاعة التفتيش في ظل أحكام الاختصاص المحلي، بحيث أجاز بتمديد التفتيش من منظومة معلوماتية إلى أخرى، فإذا كانت الأسباب تدعوا إلى الاعتقاد بان المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وإن هذه المعطيات يمكن الدخول انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة المختصة مسبقا[4].

غير أن المشكل يبقى مطروح إذا كانت المنظومة المعلوماتية المراد تمديد التفتيش إليها خارج الإقليم الوطني، فلا يمكن تمديد التفتيش إلا بتقديم طلب مساعدة قضائية دولية للدولة التي توجد فيها المنظومة المعلوماتية، وقد تستجيب الدول للطلب كما قد ترفضه و ذلك حسب الاتفاقيات الدولية المبرمة في مجال مكافحة هذا النوع من الجرائم و وفقا لمبدأ المعاملة بالمثل[5].

الخاتمة:

---

[1] - المادة 40 مكرر 3 من القانون نفسه.

[2] - المادة 40 مكرر 5 من القانون نفسه.

[3] - المادة 40 مكرر 4 من القانون نفسه.

[4] - المادة 05 من القانون 04/09 المؤرخ في 14 شعبان 1430 الموافق ل 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، ج.ر. عدد 47، غشت 2009، ص. 05.

[5] - المادة 16 من نفس القانون.

تظهر أهمية تحديد الاختصاص القضائي للجريمة المعلوماتية نظرا خطورتها من جهة، ومن طبيعتها من جهة أخرى، كونها سهلة الوقوع من أشخاص يحملون جنسيات مختلفة وتمتد عناصرها المادية وسلوكياتها الإجرامية بين أكثر من دولة، وفي فترات زمنية قصيرة جدا، وهذا و يبقى هناك عجز في معالجة جميع القضايا في هذا الشأن ما لم يكن هناك تعاون دولي جاد وسريع ،وكذا وجوب إعداد تشريعات وطنية لتجريم الظاهرة، ومنها إمكانية معاقبة كل من يتم القبض عليه على إقليم الدولة دون مراعاة لجنسيته أو مكان وقوع الفعل الإجرامي.

والملاحظ أن اغلب التشريعات الوضعية لم تنص قواعد الاختصاص القضائي بالنسبة لهذا النوع من الجرائم بالرغم من أهميته لذلك ونرى وجوب النص عليها عند إعداد قانون خاص بمعالجة الجريمة المعلوماتية وجرائم الكمبيوتر والانترنت، ونحن نعتقد أن الجريمة المعلوماتية لا تقل أهمية عن باقي الجرائم الأخرى الخطيرة كونها تهدد امن وسلامة المجتمع الدولي من خلال اهتزاز الثقة في التعامل بالبيانات والمعطيات على الشبكة العنكبوتية مما يهدد الاقتصاد العالمي الذي يشهد وتيرة متصاعدة خصوص في المجال المالي والبنكي، وعليه أصبح من الضروري معاقبة الجناة في أي إقليم يتم فيه القبض عليه دون مراعاة لجنسيته أو مكان ارتكاب جريمته لارتكابه جريمة عالمية.

كما يجب وتضافر التعاون الدولي و الجهود من أجل تحديد قواعد خاصة لهذا النوع من الجرائم، و ذلك بغض النظر عن العقبات التي تعترض الدول من أجل هذا و التي من أهمها عدم وجود اتفاق عام بين الدول على مفهوم الجرائم الإلكترونية ، عدم وجود توافق بين قوانين الإجراءات الجنائية للدول بشان التحقيق في تلك الجرائم ، والنقص الظاهر في مجال الخبرة لدي الشرطة وجهات القضائية . لأن قصور التشريعات الداخلية من جهة و غياب التنسيق الدولي الذي يعالج سبل التصدي لهذه الجرائم من جهة أخرى ، حيث لا تستطيع أية دولة مجابهة الجريمة الإلكترونية و إشكالية الإختصاص التي تطرحها و التي تتخطى إمكانياتها القضائية بمنأى و بمعزل دون وضع نظام تعاون دولي فعال من أجل إزالة مختلف هذه الإشكاليات ، الأمر الذي أصبح يفرض على المجتمع الدولي البحث عن وسائل أكثر ملائمة لطبيعتها و تضييق الثغرات القانونية التي برع مرتكبوها في استغلالها للتهرب من العقاب و لنشر نشاطهم في مناطق مختلفة من أنحاء العالم.

الإثبات الجنائي بالدليل الرقمي (دراسة تحليلية مقارنة)

Forensic evidence in digital evidence (a comparative analytical study)

أ. محمد ساير المحمد
كلية الحقوق
جامعة دمشق

مقدمة :

أدى التطور التكلوجي الكبير في هذا العصر إلى إنتاج وسائل تقنية حديثة كأجهزة الحاسب الآلي وشبكة الإنترنيت ، وعملت تلك الوسائل على تغيير حياة الأفراد اليومية وعلاقاتهم الإجتماعية حيث أصبح الإعتماد عليها كبيراً في شتى مجالات الحياة ، وقد رافق هذا التطور ظهور جرائم مستحدثة لم تكن معروفة من قبل والتي اصطلح على تسميتها من قبل المتخصصين والباحثين بالجرائم المعلوماتية والتي أصبحت في الوقت الحاضر خطراً يهدد الأفراد والدول في جميع المجالات ولمكافحة الجريمة المعلوماتية أصبح من الضروري إيجاد وسائل جديدة تختلف جذرياً عن ما يتم استعماله في مكافحة الجرائم التقليدية وذلك بسبب عجز إجراءات التحقيق التقليدية عن مجاراة نسق تطور هذه الجريمة ، بالإضافة إلى عجز الأدلة الجنائية المادية في إثبات وقوعها وهو ما توجب على جهات التحقيق الإعتماد على أدلة جديدة في مجال الإثبات الجنائي تعرف بالأدلة الجنائية الرقمية[1]لذلك سنتحدث في هذا البحث عن مفهوم هذه الأدلة وماهيتها وطبيعتها ، بالإضافة إلى حجيتها بالإثبات وموقف القانون السوري وبعض القوانين الأخرى منها، وإجراءات جمع هذه الأدلة وتقييم مدى كفاية الإجراءات المنصوص عليها في القانون لجمع الأدلة الرقمية وضبطها ، وسنصل في نهاية هذا البحث إلى مجموعة من النتائج والمقترحات علنا نصل إلى أحكام قانونية جديدة تحكم هذه الأدلة وتلائمها .

إشكالية البحث :

[1]- طاهري عبد المطلب : الإثبات الجنائي بالأدلة الرقمية ، مذكرة مكلة لنيل شهادة الماستر في الحقوق ، جامعة المسيلة ، كلية الحقوق والعلوم السياسية ، قسم الحقوق ، 2015 ، ص 1 .

تكمن إشكالية هذا البحث في مدىقابلية الدليل الرقمي لإستخدامه في إثبات الجرائم أمام القضاء وجهات التحقيق ، ونحن نسعى من خلال هذا البحث للإجابة على التساؤلات التالية :

1 -ما هو تعريف الدليل الرقمي ؟

2 - هل يتميز الدليل الرقمي عن الدليل المادي ؟

3 - ماهي حجية الدليل الرقمي في الإثبات الجنائي ؟

4 - هل القواعد العامة في إجراءات جمع الأدلة تنطبق على جمع الأدلة الرقمية ؟

أهمية البحث :

يعد موضوع الإثبات الجنائي بالدليل الرقمي من الموضوعات الجديدة والمهمة في إطار القسم الإجرائي من القانون الجزائي ، وهو من الموضوعات التي لم تنل حظها من البحث والتمحيص في الفقه الجزائي ، إذ أن أغلب الدراسات المنشورة عن الجريمة المعلوماتية تتعلق بالجانب الموضوعي منها دون الغوص في الجانب الإجرائي وجانب الإثبات بحثاً وشرحاً .

أهداف البحث :

من الأهداف التي يسعى إليها هذا البحث :

1 - التعريف بالدليل الرقمي ومعرفة ماهيته وخصائصه عند بعض الشراح .

2 - توضيح موقف القانون السوري والمقارن من الدليل الرقمي وحجيته في الإثبات الجنائي .

3 - التعرف على إجراءات جمع الأدلة الرقمية ومدى انطباق الإجراءات التقليدية عليها .

منهج البحث :

اعتمدنا في هذا البحث على المنهج التحليلي من خلال بيان نصوص القانون السوري المتعلقة بالدليل الرقمي وتحليل أحكامها وشرحها ، كما اعتمدنا على الدراسة المقارنة من خلال مقارنة أحكام القانون السوري مع بعض القوانين التي تتبنى أنظمة أخرى في الإثبات تختلف عنه إذا لزم الأمر .

خطة البحث :

المطلب الأول : مفهوم الأدلة الرقمية وحجيتها

المطلب الثاني : طرق وإجراءات جمع الأدلة الرقمية

المطلب الأول :مفهوم الأدلة الرقمية وحجيتها

على الرغم من الجانب المشرق الذي أفرزته الثورة المعلوماتية التي شهدها العالم في العصر الحديث إلا أنها أفرزت جوانب سلبية متمثلة بالاستعمال غير المشروع للوسائل الإلكترونية

والتي نجم عنها أنماط مستحدثة من الجرائم اصطلح على تسميتها ب " الجرائم الإلكترونية " ، ولكشف هذه الجرائم كان لا بد من الإستغناء عن الأدلة التقليدية والإستعانة بالأدلة الرقمية التي هي نتاج الأساليب العلمية الحديثة في التحقيق الجنائي ، ويتضح أثر الأدلة الرقمية في تحجيم الجريمة الإلكترونية والحد من خطورتها عن طرق إتاحة الوسائل لكشفها[1]، ذلك الأثر الذي لا تستطيع الأدلة التقليدية أن تقوم به .

وعلى هذا سندرس في هذا المطلب مفهوم الأدلة الرقمية وحجيتها على النحو التالي :

الفرع الأول : ماهية الدليل الرقمي :

سندرس في هذا الفرع أولاً التعريف بالدليل الرقمي وثانياً خصائص الدليل الرقمي في مجال التحقيق الجنائي .

أولاً : التعريف بالدليل الرقمي :

عرف القانون السوري الدليل الرقمي في المادة الأولى من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية (القانون رقم 17 لعام 2012) على أنه **البيانات الرقمية المخزنة في الأجهزة الحاسوبية أو المنظومات المعلوماتية أو المنقولة بواسطتها والتي يمكن استخدامها في إثبات أو نفي جريمة معلوماتية.**

وسنستعرض بعض التعريفات التي أتى بها فقهاء القانون الجزائي فقد عُرف بأنه الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها أو تحليلها باستخدام برامج وتطبيقات تكنلوجية خاصة ، ويتم تقديمها كدليل يمكن الإعتماد عليه أمام القضاء . كما عُرف بأنه ذبذبات أو نبضات الكترونية مسجلة على وسائط أو دعائم الكترونية والتي تم الحصول عليها بواسطة التقنية الإلكترونية من معطيات الحاسوب وشبكة الإنترنيت من خلال إجراءات قانونية لتقديمها للقضاء كدليل الكتروني جنائي يصلح لإثبات الجريمة.

[1]- رفاه خضير جياد العارضي : الدليل الإلكتروني وأثره في مجال نظرية الإثبات الجنائي ، دراسة مقارنة ، منشوات زين الحقوقية بيروت ، لبنان ، ص 9 .

وبناء على ما سبق[1] ، يمكن لنا القول بأن هذه التعريفات قد جانبت الصواب حين عرفت الدليل الرقمي من حيث تكوينه فقط ، بأنه عبارة عن نبضات مغناطيسية أو كهربائية تشكل لنا معلومات أو بيانات مختلفة ، وهذه التعريفات اعتمدت فقط على الأدلة المستخلصة من الحاسب الآلي أو شبكة الإنترنيت ، في حين أنه يمكن الحصول على الأدلة الرقمية من خلال الهواتف الذكية أو أجهزة تحديد الموقع (GPS) أو أي جهاز أخر يتميز بنفس الخصائص ، كما يؤخذ على تعريف القانون السوري للدليل الرقمي بأنه قصر أثره على إثبات الجريمة المعلوماتية في حين يمكن أن يستخدم في إثبات جريمة معلوماتية أو تقليدية على حد سواء . والتعريف الذي نراه صحيح وشامل للدليل الرقمي هو تعريف الفقيه البريطاني (كيسي) فهو يُعرف الأدلة الجنائية الرقمية بأنها تشمل جميع البيانات الرقمية التي يمكن أن تثبت بأن هناك جريمة قد ارتُكبت أو توجد علاقة بين الجريمة والجاني أو بين الجريمة والمجني عليه ، والبيانات الرقمية هي مجموعة الارقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة ، الرسومات ، الخرائط ، الصوت أو الصورة [2] .

ثانياً : خصائص الدليل الرقمي في مجال الإثبات الجنائي :

يمتاز الدليل الرقمي عن الدليل المادي المأخوذ من مسرح الجريمة التقليدي بما يلي[3] :

1 - طريقة نسخ الدليل الرقمي من أجهزة الكمبيوتر تقلل أو تعدم تقريباً مخاطر إتلاف الدليل الأصلي حيث تتطابق طريقة النسخ مع طريقة الإنشاء .

2 - باستخدام التطبيقات والبرامج الصحيحة ، يكون من السهولة تحديد ما إذا كان الدليل الرقمي قد تم العبث به أو تعديله وذلك لإمكانية مقارنته بالأصل .

3 - توجد صعوبة في محو الدليل الرقمي من قبل الجاني ، حتى في حال محاولة ذلك يمكن استرجاع الدليل الرقمي من جديد .

---

[1]. م . د نضال ياسين الحاج حمو : دور الدليل الإلكتروني في الإثبات الجنائي ، دراسة تحليلية ، مجلة جامعة تكريت للعلوم القانونية والسياسية ، المجلد 1 ، السنة 5 ، العدد 19 ، ص 181 .

[2] -اللواء د . محمد الأمين البشري : الأدلة الجنائية الرقمية (أهميتها ودورها في الإثبات) ، الإمارات العربية المتحدة ، ص 109 .

[3] - د . مصطفى محمد موسى : التحقيق الجنائي في الجرائم الإلكترونية ، الطبعة الأولى ، مطابع الشرطة ، القاهرة ، 2009
ص 218 - 219 .

4 - إن محاولة الجاني محو الدليل الرقمي يمكن تسجيلها كدليل ضده ، حيث إن نسخة من فعل الجاني لمحو الدليل يمكن استخلاصها لاحقاً كدليل إدانة ضده .

5 - إن اتساع مسرح الجريمة الإلكترونية على مستوى العالم ، يجعل بإمكان مستغلي الدليل تبادل المعرفة بسرعة عالية وبمناطق مختلفة من العالم ، مما يسهم في تسهيل كشف الجناة بسرعة .

6 - قابليته للتخزين بسعة تخزينية عالية ، فآلة الفيديو الرقمية يمكنها تخزين مئات الصور ، ومشغل وسائط صغير يمكنه تخزين مكتبة تضم العديد من الكتب الإلكترونية التي تصلح كدليل .

7 - يمكن من خلال الدليل الرقمي رصد المعلومات عن الجاني وتحليلها في نفس الوقت ، فالدليل الرقمي يمكنه أن يسجل تحركات الفرد ، كما يسجل عاداته وسلوكياته وبعض الأمور الشخصية عنه لذا فإن الجهة المختصة بالبحث الجنائي قد تجد غايتها بسهولة أكثر من الدليل المادي .

الفرع الثاني : حجية الدليل الرقمي :

يختلف موقف القوانين من حجية الدليل الرقمي من دولة لأخرى حسب نظام الإثبات الذي تعتنقه كل دولة ، ووفقاً لما كشفت عنه الدراسات المقارنة في هذا المجال فإنه يوجد نظامين : نظام الإثبات المقيد ونظام الإثبات الحر ، ولن نتعرض في هذا الفرع لشرح هذين النظامين وإنما سوف نقتصر على ذكر أمثلة على الدول التي تعتنق كل من هذين النظامين مع بيان موقف القانون السوري ، وعلى ذلك سوف ندرس أولاً موقف القانون الإنكليزي من الدليل الرقمي وثانياً موقف القانون الفرنسي من الدليل الرقمي وثالثاً موقف القانون السوري من الدليل الرقمي .

أولاً : موقف القانون الإنكليزي من الدليل الرقمي :

أخذت إنكلترا بنظام الإثبات المقيد وتعتبر إنكلترا من أولى الدول التي أصدرت قانوناً خاصاً بجرائم الحاسب الآلي (قانون إساءة استخدام الحاسب الآلي الصادر عام 1990م) ، وهذا القانون لم يتطرق لقبول الأدلة الناتجة عن استخدام الحاسب الآلي وذلك بسبب أن قانون البوليس والإثبات الجنائي الصادر في سنة 1984م قد احتوى تنظيماً محدداً لقواعد قبول الأدلة الرقمية .

ومن خلال النظر إلى نصوص قانون البوليس والإثبات الجنائي نجد أن الأدلة الناتجة عن استخدام الحاسب الآلي لا تقبل كدليل إلا إذا استكملت اختبارات الثقة المنصوص عليها في هذا القانون ، فلا يُقبل هذا الدليل إذا وُجِد سبب معقول يدعو للإعتقاد بأن هذا الدليل غير دقيق أو بياناته غير سليمة ، أو أن الحاسب الآلي الذي استُخرج منه الدليل الرقمي لا يعمل

بكفاءة وبصورة سليمة ، وقد اقترح بعض الفقهاء الإنكليز أيضاً حالة ثالثة وهي استخدام الحاسب الآلي بشكل غير مصرح به ، وبالتالي عدم قبول الأدلة الناتجة عن هذا الإستخدام[1].

ثانياً : موقف القانون الفرنسي من الدليل الرقمي :

يمكن القول أن الدليل الرقمي لا يثير أي صعوبة في القانون الفرنسي ما دام المشرع الفرنسي قد أخذ بنظام الإثبات الحر ، وهذا على عكس التشريعات التي تأخذ بنظام الإثبات المقيد مثل إنكلترا (كما ذكرنا) والتي أَلزمت بإحترام طرق تقديم الدليل الرقمي وإخضاعه لإختبارات الثقة التي تحدثنا عنها .

وقد أراد الفقه الفرنسي التوسع في قبول الأدلة الجنائية الرقمية أمام القضاء ، وذلك عن طرق قبول الأدلة الناتجة عن أجهزة التصوير وكاميرات المراقبة والرادارات ، وأجهزة تسجيل الأصوات وغيرها ، وقد قضت محكمة النقض الفرنسية في قرار صادر لها بتاريخ 1984/4/28م أن أشرطة التسجيل الممغنطة يمكن أن تكون صالحة أمام القضاء الجزائي .

وعليه فالتسجيل الصوتي إلكترونياً بواسطة أجهزة خاصة بذلك يصلح لأن يكون دليل إثبات في فرنسا فهو لا يحتمل الخطأ ويصعب التلاعب فيه ، ويمكن للخبراء الفنيين أن يكتشفوا أي تلاعب فيه بواسطة أجهزة تقنية عالية الكفاءة .

وكذلك فإن الأدلة الناتجة عن استخدام الحاسب الآلي تميز بأن أي محاولة لحذف أو محو الدليل يُسجل كدليل ضد الجاني ويعتبر قرينة عليه ، وهذا من الميزات التي يتمتع بها الدليل الرقمي مقارنة بالأدلة التقليدية والتي ذكرناها سابقاً ، لكن المشرع الفرنسي مع ذلك اشترط للإعتداد بالأدلة الرقمية أن يتم الحصول عليها بطريقة مشروعة ونزيهة ، وأن يتم مناقشتها حضورياً من قبل أطراف الدعوى العامة (وطبعاً هذا الأمر ينطبق على أي دليل) .

ثالثا : موقف القانون السوري من الدليل الرقمي :

حذى المشرع السوري حذو المشرع الفرنسي وسار على خطاه آخذاً بنظام الإثبات الحر فالقاضي الجزائي في سوريا حر في الأخذ بالدليل الذي يراه مناسباً في تكوين قناعته الوجدانية وإهمال مالا يلزم ، وعلى ذلك أعطى القانون السوري سلطة تقديرية للمحكمة في قبول الدليل الرقمي أو رفضه حسب ما تراه مناسباً ، كما هو مذكور في المادة 25 من قانون تنظيم التواصل على الشبكة ومكافحة

[1] - طاهري عبد المطلب : الإثبات الجنائي بالأدلة الرقمية ، المرجع السابق ، ص 61

الجريمة المعلوماتية (الصادر بالمرسوم التشريعي رقم 17 لعام 2012) والتي نصت بدورها على شروط قبول الدليل الرقمي في الإثبات وهذه الشروط هي :

1- أن تكون الأجهزة الحاسوبية أو المنظومات المعلوماتية المستمد منها الدليل تعمل على نحو سليم .

2 - ألا يطرأ على الدليل المقدم إلى المحكمة أي تغيير خلال مدة حفظه .

والأصل صحة الدليل الرقمي أي أن المشرع السوري افترض أن الدليل مستوفياً الشرطين السابقين لكن هذا الإفتراض قابل لإثبات العكس .

وبذلك انتهينا من دراسة مفهوم الأدلة الرقمية وحجيتها في (المطلب الأول) وسننتقل بعد ذلك لدراسة طرق وإجراءات جمع الأدلة الرقمية في (المطلب الثاني) .

المطلب الثاني :طرق وإجراءات جمع الأدلة الرقمية

يتطلب التعامل مع مسرح الجريمة ، سواء أكان مسرحاً مادياً أم مسرحاً الكترونياً ، إجراءات روتينية معينة منصوص عليها في القانون لحماية الدليل والحفاظ على قيمته ، إلا أن هذه الإجراءات تختلف بين مسرح الجريمة المادي ومسرح الجريمة الإلكتروني ، ذلك أن التطبيقات أو البرامج والبيانات الرقمية تعد عناصر أساسية يتعين على الأجهزة المختصة بالتحقيق مع الإستعانة بالخبرة الفنية جمعها واستخلاصها ، وإن هذه الجهات ستجد صعوبة في جمع الأدلة الرقمية باستخدام الوسائل العادية (التقليدية) لأن عالم الإلكترونيات مختلف ، ولأن الحقيقة إذا كانت قابلة للتطور فإن الدليل الذي يكشف هذه الحقيقة لا بد أن يكون متطوراً ولا بد أن تكون وسائل التعامل معه متطورة أيضاً مما يتفق مع هذا الدليل[1] .

وعلى هذا سندرس في هذا المطلب طرق وإجراءات جمع الأدلة الرقمية على النحو التالي :

الفرع الأول : التفتيش والضبط :

يهدف التفتيش إلى البحث عن أدلة الجريمة وما نجم عنها وكل ما يفيد في كشف حقيقتها ومعرفة هوية مرتكبيها ومكان وجودهم ، أي البحث عن السر الذي يتعلق بالجريمة ، وهو السر الذي يحتفظ فيه الشخص لنفسه ويحرص على عدم إطلاع الناس عليه ، والضبط معناه وضع

---

[1]- رفاه خضير جياد العارضي : الدليل الإلكتروني وأثره في مجال نظرية الإثبات الجنائي ، المرجع السابق ، ص 111 .

اليد على شيء يتعلق بجريمة وقعت ، فضبط الأشياء المتعلقة بالجريمة هي الغاية الأساسية من التفتيش [1] .

وسندرس في هذا الفرع أولاً طبيعة إجراءات التفتيش والضبط في النظم الإلكترونية وثانياً الإختصاص المكاني في البحث عن الدليل الرقمي .

أولاً : طبيعة إجراءات التفتيش والضبط في النظم الإلكترونية :

إن إجراءات التفتيش والضبط المتعلقة بنظم الحاسوب ، يسهل إجراؤها على النظم المادية للحاسوب وتنطبق عليها القواعد التقليدية ، أما بالنسبة للمكونات غير المادية (المعنوية) للحاسوب فالأمر قد يثير بعض الصعوبة ، فالمقصود بالتفتيش عن الأدلة الرقمية هو التفتيش عن المعطيات غير المادية المخزنة في الجهاز ، أو المخزنة في الأقراص ، أو البحث في النظم المعلوماتية عبر الشبكات الإلكترونية بحثاً عن شيء يتصل بالجريمة[2].

وموقف المشرع السوري من هذه المسألة نستخلصه من أحكام قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية (القانون رقم 17 لعام 2012) في الفقرة ب من المادة 26 منه ، والتي تنص على :

تعد البرمجيات الحاسوبية من الأشياء المادية التي يجوز تفتيشها وضبطها ، وفق القواعد المنصوص عليها في قانون أصول المحاكمات الجزائية .

وحسب التعليمات التنفيذية لهذه المادة فإن الغرض من هذه الفقرة هو النص على أن البرمجيات الحاسوبية ، إلى جانب الأشياء المادية الأخرى تكون خاضعة للتفتيش والضبط .

وإذا كان الأمر مقبول من الناحية النظرية ، إلا أن ضبط مكونات الحاسوب المعنوية بعد تفتيشها غير ممكن إلا إذا حُولت إلى كيانات مادية عن طريق مخرجات الحاسوب المختلفة ، كطباعتها أو نقلها على أقراص أو تسجيلها على أي دعامة أخرى ، وبذلك يمكن ضبط مكونات الحاسوب بكاملها كدليل على الجريمة [3] ، ويتضح مما سبق أن معطيات الحاسوب غير المادية

---

[1]- د . بارعة القدسي : أصول المحاكمات الجزائية ، الجزء الثاني (سير الدعوى العامة) ، منشورات جامعة دمشق ، كلية الحقوق 2011 ، ص 185 - ص 192 .

[2]- المحامي خالد عياد الحلبي : إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنيت ، دار الثقافة للنشر والتوزيع ، الأردن الطبعة الأولى ، 2011 ، ص 151 - ص 157 .

[3]-جلال الزعبي وأسامة المناعسة وصايل الهوواشة : جرائم الحاسوب والإنترنيت ، دار وائل ،عمان ، 2001 ، ص 266 .

تخضع للتفتيش ، لأنها عبارة عن ذبذبات إلكترونية أو موجات كهرومغناطيسية قابلة للتخزين في الجهاز أو التخزين على الأقراص ، وإنها ما دامت كذلك فهي أشياء مادية محسوسة تخضع للتفتيش ويمكن ضبطها[1].

ويرى بعض الفقهاء في فرنسا أن النبضات أو الإشارات الإلكترونية الممغنطة لا تعتبر من قبيل الأشياء المادية المحسوسة بالمعنى المألوف للمصطلح وبالتالي لا يمكن ضبطها [2] .

ونحن نرد على هذا الرأي من خلال موقف المشرع السوري في المادة 26 المذكورة آنفاً ، وهو الرأي الذي نتبناه .

ثانياً : الإختصاص المكاني في البحث عن الدليل الرقمي :

يتحدد الإختصاص المكاني في المسائل الجزائية في سوريا بإحدى المعايير التالية : إما مكان وقوع الجريمة ، أو موطن المدعى عليه ، أو مكان إلقاء القبض عليه ، وذلك بحسب المادة 3 من قانون أصول المحاكمات الجزائية السوري ، والتي تقابلها المادة 9 من قانون أصول المحاكمات الجزائية اللبناني وتتطابق معها .

فالمحافظ يقوم بوظائفه ضمن الحدود الإدارية لمحافظته ، وضابط الشرطة يقوم بوظائفه ضمن الحدود الإدارية للقسم الذي يتبع له ، فإذا تجاوزوا حدود إختصاصهم المكاني يصبح أي واحد منهم كفرد عادي وتكون إجراءاته باطلة (بإستثناء حالة الضرورة) ، فليس لهم مباشرة إجراءاتهم خارج حدود الإختصاص المكاني للجهة التي هم معينون لها[3].

وتجدر الملاحظة إلى أن القانون خول بعض الضباط العدليين الحق بالقيام بوظائفهم في جميع أنحاء الجمهورية العربية السورية نظراً لطبيعة وظائفهم ، كالنائب العام للجمهورية ، وقائد قوى الأمن الداخلي ، ورئيس شعبة الأمن السياسي ، ورئيس شعبة الأمن الجنائي[4].

---

[1] - المحامي خالد عياد الحلبي : إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنيت ، المرجع السابق ، ص 158 .

[2] - د . عبد الله حسين محمود : سرقة المعلومات المخزنة بالحاسوب ، رسالة دكتوراه ، جامعة عين شمس ، مصر، 2001،ص605.

[3] - د . بارعة القدسي : أصول المحاكمات الجزائية ، الجزء الثاني (سير الدعوى العامة) ، المرجع السابق ، ص 72 .

[4]- - د . حسن خوخدار : أصول المحاكمات الجزائية ، الجزء الثاني (المراحل الإجرائية التي تمر بها التهمة) ، منشورات جامعة دمشق ، 1992 ، ص 8 .

تأليف مجموعة من الباحثين

أما فيما يتعلق بالجريمة المعلوماتية فبحسب الفقرة 1 من المادة 24 من قانون مكافحة الجريمة المعلوماتية السوري السالف ذكره فإنه **تحدث في وزارة الداخلية ضابطة عدلية مختصة تكلف بإستقصاء الجرائم المعلوماتية وجمع أدلتها الرقمية ، والقبض على فاعليها وإحالتهم على المحاكم الموكول إليها أمر معاقبتهم .**

وتنفيذاً لهذه الفقرة فقد أصدر السيد وزير الداخلية القرار رقم 564 / ق تاريخ 22 / 3 / 2012 المتضمن إحداث فرع خاص في إدارة الأمن الجنائي يسمى (فرع مكافحة الجريمة المعلوماتية) لمكافحة هذه الجرائم وجمع أدلتها الرقمية ، والقبض على فاعليها وتقديمهم إلى القضاء[1].

ويشمل اختصاص فرع مكافحة الجريمة المعلوماتية السوري جميع أنحاء الجمهورية العربية السورية ونحن نأمل بإحداث فرع في كل محافظة لدى إدارة الأمن الجنائي مختص بمكافحة الجريمة المعلوماتية ، حتى يتسنى تقديم الشكوى بيسر وسهولة ، وحتى يتمكن أعضاء الفرع من مكافحة الجريمة وضبط أدلتها بالسرعة القصوى .

أما الجزائر فقد قامت بإنشاء مركز لمكافحة جرائم الإنترنيت على مستوى الدرك الوطني ، وبدأ مهامه في أواخر عام 2006[2].

الفرع الثاني : الإستعانة بالخبراء :

إزدادت أهمية الخبرة في العصر الحاضر نتيجة تقدم العلوم وتشعبها ، وقد انعكس ذلك على العلوم الجنائية وما يتصل بها ، فعند وقوع الجريمة لابد من الكشف عن أدلتها التي تساعد على كشف حقيقة الجريمة ومعرفة مرتكبيها وكيفية ارتكابها ، وكثيراً ما يتطلب فحص هذه الأدلة معرفة عالية وخبرة فنية لا يملك مثلها القاضي أو المحقق ، مما يضطره إلى الإستعانة بشخص إختصاصي أو فني لبيان حقيقتها [3].

وعلى ذلك سندرس في هذا الفرع أولاً إلزامية اللجوء إلى الخبرة وثانياًدور الخبراء في حفظ الدليل الرقمي.

أولاً : إلزامية اللجوء إلى الخبرة :

[1]- - د . طارق الخن : جرائم المعلوماتية ، منشورات الجامعة الإفتراضية السورية ، 2018 ، ص 117 .

[2]- نبيلة هبة هروال : الجوانب الإجرائية لجرائم الإنترنيت في مرحلة جمع الإستدلالات ، دار الفكر الجامعي ، الإسكندرية الطبعة الأولى ، 2007 ، ص 145 .

[3]- المستشار أنس كيلاني : موسوعة الإثبات في القضايا المدنية والتجارية والشرعية ، الطبعة الأولى ، 1991 ، ص 914 .

إن السؤال الذي يمكن طرحه هنا هو : هل القاضي أو المحقق ملزم باللجوء إلى الخبرة ؟
الأصل في هذه المسألة أن الأمر جوازي بالنسبة للقاضي أو المحقق ، فهو له سلطة تقديرية في أن ينتدب خبيراً أم لا ، كما له أن يرفض انتداب خبير عندما يتعلق الأمر بوصف أمور واضحة، فعندها يقرر بنفسه الحقيقة من خلال المشاهدات والأدلة الأخرى ، فهو الخبير الأعلى في كل ما يستطيع معرفته بنفسه ، أما إذا كان الأمر يتعلق بمسألة فنية بحتة ، فإن القاضي أو المحقق يصبح ملزماً باللجوء إلى الخبرة [1] ، وقد حكمت محكمة النقض السورية بأنه **ليس** للمحكمة أن تفصل في أمور فنية وعلمية لا يستوي في معرفتها ذوي الإختصاص مع غيرهم بل عليها أن تستعين بالخبراء في كل علم لتحقيق ما هو داخل بخبرتهم[2].
وقانون أصول المحاكمات الجزائية السوري لم يتضمن أحكاماً مستقلة بالخبرة ، وإنما اعترف بها ضمن الإجراءات التي يستطيع قاضي التحقيق اللجوء لها إذا رأى ضرورة لذلك وذلك في المادة 39 والمادة 40 منه ، وكذلك الحال بالنسبة لقانون أصول المحاكمات الجزائية اللبناني في المادة 34 والمادة 74 منه .
أما فيما يتعلق بقانون مكافحة الجريمة المعلوماتية السوري فقد نص في المادة 24 فقرة ب منه على أن تستعين الضابطة العدلية المختصة بخبراء دائمين ومؤقتين ، من وزارة الدفاع ووزارة العدل، ووزارة الإتصالات والتقانة ، لتنفيذ المهام الموكلة إليها ، ويقسم هؤلاء الخبراء اليمين القانونية .
وفحوى هذه المادة تدل على إلزامية اللجوء إلى الخبرة في مجال التحقيق في الجرائم المعلوماتية .

ثانياً : دور الخبير في حفظ الدليل الرقمي :

في إطار حفظ الأدلة الرقمية يمكن التمييز بين الأدلة التي يُلزم التحفظ عليها داخل الحاسوب ، وبين الأدلة التي تنتمي إلى العالم الإفتراضي ، ومع ذلك يمكن اللجوء إلى إخراجها من الحاسوب إلى العالم المادي ليتم التعامل معها كمخرجات يقبلها القضاء كأدلة كاملة في الجريمة وتساعد على الإدانة أو البراءة كما ذكرنا سابقاً .

[1] - د . بارعة القدسي : أصول المحاكمات الجزائية ، الجزء الثاني (سير الدعوى العامة) ، ص 143 .

[2] مجموعة القواعد القانونية التي قررتها محكمة النقض السورية بين عامي 1949 و1968 ، رقم القاعدة 56، ص 32 .

وإن التحفظ على الدليل الرقمي داخل الحاسوب يحتاج إلى رصد دقيق لمدى صحة البيانات التي يحتوي عليها الحاسوب ، وهذا الأمر يتطلب من الخبير الكشف عن حالة الحاسوب وجاهزيته، لا سيما من حيث الخلل أو العطب في الجهاز ، كما لو كان الجهاز مصاباً بالفيروسات ، إذ يكفي أن يوجد فيروس واحد في الجهاز حتى يتم التشكيك في صحة الدليل المستخرج منه ، كما يجب على الخبير حفظ الدليل وتحريزه في بيئة لا تفسده ، وذلك بإتباع السلامة المنهجية الخاصة بحفظ الدليل الرقمي .

أما بالنسبة لعملية حفظ الأدلة في العالم الرقمي ، فذلك يتطلب من الخبير رصد موقع الإنترنيت أو البيانات التي تشير إلى الجريمة التي تكون في مظاهر مختلفة الأشكال ، كما لو كان هناك جريمة قدح وذم [1] في إحدى غرف الدردشة ، ففي هذه الحالة يتم اللجوء لذاكرة الخادم الذي يتولى ربط هذه الغرف عبر العالم الرقمي ، لكي يتم التوصل لتحديد موضوع القدح والذم وإثبات هذه الجريمة[2].

ودرءاً للمشاكل التي قد تنجم عن حفظ الدليل الرقمي فإن محاكم العديد من دول العالم المعاصر (فرنسا ، بريطانيا) لجألت إلى إمكانية إدارتها رقمياً ، بحيث يتم تسليمها إلى إدارة متخصصة تتولى حفظ الأدلة الرقمية لحين عرضها على القضاء كلما تطلب الأمر ذلك [3] ، ونحن بدورنا نتمنى اللجوء إلى هذه التقنية في سوريا وإلى تقنيات حديثة أخرى متبعة في الدول المتقدمة حتى يتسنى للأجهزة المختصة في سوريا مواكبة التطور والحداثة في هذا المجال .

خاتمة

تبين لنا من خلال عرض أفكار هذا البحث أن ثمة غموض في مفهوم الدليل الرقمي بشكل عام وهذا راجع إلى قلة الندوات التي تتحدث عن هذا الموضوع ، كما أن ضعف استخدام الدليل الرقمي في الواقع العملي يرجع إلى حداثته وجهل الكثيرين بأهميته ومزاياه ، كما تبين لنا عجز القواعد العامة التي تحكم إجراءات التحقيق التقليدية عن مجاراه الأدلة الرقمية وإجراءات جمعها

---

1 - عاقب قانون العقوبات السوري على هذه الجريمة في المواد ((568 - 572)) في الباب الثامن ((في الجنايات والجنح التي تقع على الأشخاص)) .

2 - رفاه خضير جياد العارضي : الدليل الإلكتروني وأثره في مجال نظرية الإثبات الجنائي ، المرجع السابق ، ص 179.

3 - رفاه خضير جياد العارضي : الدليل الإلكتروني وأثره في مجال نظرية الإثبات الجنائي ، المرجع السابق ، ص 180 .

نظراً لخصوصية هذه الأدلة من حيث وجودها في العالم الإفتراضي ، ونحن نخلص من وراء ذلك إلى مجموعة من المقترحات نبينها على الوجه الآتي :

1 - عقد الندوات والمحاضرات والبرامج التعريفية عن موضوع الدليل الرقمي ، وإدخال مقرر اسمه (التحقيق الجنائي في الجرائم المعلوماتية) ضمن الخطة الدراسية لكليات الحقوق .

2 - إقامة دورات فنية متخصصة في مجال التعامل مع الأدلة الرقمية تخص القضاة وضباط الشرطة والخبراء المتخصصين في الجرائم المعلوماتية .

3 - إحداث أكثر من فرع لمكافحة الجرائم المعلوماتية في البلاد حتى يتسنى للضابطة العدلية القيام بدورها الأمثل بقمع الجريمة المعلوماتية والحد منها .

4 -تكثيف الجهود الرامية إلى التعاون الدولي في مكافحة الجريمة المعلوماتية نظراً لأنها جريمة عابرة للحدود وحتى يتسنى ضبط أدلتها الرقمية بأسرع وقت ، وذلك بعقد المعاهدات والإتفاقيات الدولية المعنية بهذا الشأن .

5 - الإهتمام بالخبرة الفنية في مجال كشف الجرائم المعلوماتية بشكل عام وجمع الأدلة الرقمية بشكل خاص ، وإدخال التقنيات الحديثة التي تُعنى بحفظ الأدلة الرقمية لأطول فترة ممكنة .

المسؤولية الجزائية للشركات التجارية عن جريمتي الغش والخداع الإلكتروني

The criminal liability of commercial companies for the crimes of counterfeiting and electronic fraud

د.واسطي عبد النور أستاذ محاضر –ب-
معهد الحقوق والعلوم السياسية
المركز الجامعي بمغنية - الجزائر

مقدمة :

لا يختلف إثنان حول الدور الحثيث التي باتت تلعبه التكنولوجيات الحديثة بما فيها الأنترنيت ،فقد أصبح الفضاء المفضل للبحث، الإتصال، وحتى ممارسة الأعمال من خلال عرض السلع والخدمات. فحسب بعض التقارير والإحصائيات المنشورة فقد بلغ حجم المعاملات العالمية على الأنترنيت حوالي 35 %من حجم المعاملات الإجمالية.

فإذا كان المستهلك[1]أو مقتني السلع على العموم يحظى ببعض الحماية على الواقع الملموس، فكيف الحل على الواقع الإفتراضي؟ خاصة إذا علمنا أن رواد التجارة الإلكترونية هم عصبة من الشركات التجارية الضخمة، فمن جهة سوف يصعب التحقق من جودة وقيمة البضاعة بعدما كان اللمس والمعاينة هما السبيلان لذلك، أصبحت الصورة هي المآل الوحيد. ومن جهة أخرى وحتى ولو ثبت عدم تطابق المنتوج المقدم مع ما تسلمه المستهلك فإنه من الصعب بمكان إقامة المسؤولية والجزاء على الفاعل.

إنطلاقا من هذا الطرح وبحثا منا لمعالجة هذه الإشكالات قسمنا هذا البحث إلى قسمين، تناولنا في الأول مفهوم جريمة الغش والخداع الإلكتروني وصورها، أما الثاني نخصص لدراسة شروط قيما مسؤولية الشركات التجارية عنها.

المبحث الأول: مفهوم جريمتي الغش والخداع الإلكتروني

[1]هذا وعرف المستهلك على أنه كل شخص طبيعي أو معنوي يقتني بمقابل أو مجان سلعة أو خدمة...إلخ.فحين عرف القانون 18-05 المتعلق بالتجارة الإلكترونية المستهلك الإلكتروني في المادة 06 بأنه" كل شخص طبيعي أو معنوي يقتني بعوض أو بصفة مجانية سلعة أو خدمة عن طريق الإتصالات الإلكترونية من المورد الإلكتروني بغرض الإستخدام النهائي".

يعرف الغش أو التدليس عموماً على أنه إستعمال الطرق الإحتيالية لدفع المتعاقد على التعاقد بحيث لو علم أنه مدلس عليه لما أقدم على التعاقد. فبهذا المنطق يجب أن يتم إستعمال وسائل الإحتيال ليقع الغش والخداع وأن تكون هذه الوسائل هي الدافعة إلى التعاقد.فالغش يمكن أن يكون محله القانون ويقال له الغش نحو القانون أو محله الضريبة ويقال له الغش الضريبي أو محله السلع والبضائع وهو محل دراستنا.

فالغش قد يصيب السلع والبضائع الموجهة للإستهلاك الإنساني أو الحيواني كالمواد الغذائية أو قد يقع على المواد الطبية، كما قد يقع على المواد الصناعية أو الطبيعية التي تستعمل في إنتاج مواد أخرى. فإذا كان الغش في الإنتاج و تصنيع فإن الخداع يكون آخر مرحلة من العملية وهي التسويق والعرض للبيع وهنا يتم إستعمال الوسائل الإلكترونية لتسهيل الخداع.

المطلب الأول: تعريف جريمتي الغش والخداع الإلكتروني

يمكن تعريف الغش على أنه كل تغيير أو تسوية يقع على الجوهر أو التكوين الطبيعي لمادة أو سلعة معدة للبيع ويكون من شأن ذلك النيل من خواصها الأساسية أو إخفاء عيوبها أو إعطاء شكل أو مظهر سلعة أخرى تختلف عنها في الحقيقة، وذلك بقصد الاستفادة من الخواص المسلوبة أو الإنتفاع بالفوائد المستخلصة والحصول على فارق الثمن[1].

أما الخداع فيمكن تعرفه على إنه استعمال وسائل الإحتيال لجذب و دفع المستهلك الإلكتروني على اقتناء السلعة المعروضة أو بعبارة أخرى استعمال وسائل الإحتيال لدفع المتعاقد على التعاقد بحيث لو علم أنه تم خداعه لما أقدم على التعاقد ، حيث يعتبر هذا التعريف مستمدا من تعريف التدليس في القانون المدني[2].

بالنتيجة يمكن القول أن الغش والخداع الإلكتروني لا يختلف عن الغش والخداع العادي المعروف في القانون المدني والمعروف في قانون حماية المستهلك، فيمكننا تعريفه ببساطة هو الاحتيال في المنتوج الذي يقدم للتسويق إفتراضيا، فقد يقع هذا الإحتيال في التصنيع فيسمى غشا وقد يقع في العرض و التسويق فيسمى خداعا، ولكن الملاحظ على جريمة الغش و الخداع

---

[1] خلف أحمد محمود علي، الحماية الجنائية للمستهلك في القانون المصري والفرنسي والشريعة الإسلامية،دار الجامعة الجديدة، الإسكندرية،2005،ص 194 وما بعدها

[2]- خلف أحمد محمود علي، نفس المرجع،ص195 وما بعدها.

الإلكتروني أن الغش والخداع يكونان متلازمين لأن الغشاش يحتاج دائما إلى من يروج لمنتوجه المغشوش.

المطلب الثاني :صور جريمتي الغش والخداع الإلكتروني

أشار المشرع إلى جريمة الخداع في المادة 429 من قانون العقوبات وعدد بعض الأفعال التي تعتبر من قبل الخداع وهي الخداع في طبيعة أو الموصفات أو المكونات الجوهرية للمنتوج كما عالج المشرع جريمة الغش في بيع المواد الغذائية والطبية في المادة 431 من قانون العقوبات، ونص على مجموعة من الأفعال التي تعبر غشا. وهي على العموم الغش في مواد غذائية صالحة لتغذية الإنسان أو الحيوان أو مواد طبية أو مشروبات أو منتوجات فلاحية أو طبيعية مخصصة للإستهلاك وعرضها وبيعها مع العلم بذلك.

الفرع الأول: الغش والخداع في المواد الغذائية أو الطبية

يكون الغش إما بالإضافة أو بالإنقاص أو في التصنيع. بإضافة مواد غير مصرحة أو مواد ضعيفة القيمة مقارنة بما تم الإعلام به للمستهلك خاصة وأن العرض هنا يتم إفتراضيا لا يمكن التحقق منه، كما قد يكون الغش بإنقاص مواد أو خصائص يجب أن ترد في المنتوج أو تم التصريح والإعلام بوجودها. فحين قد يتعدى الغش إلى التحريف الكلي عند التصنيع وذلك إما مخالفة للقواعد الموضوعة مسبقا للتصنيع أو بعدم إضافة المواد التي يجب أن يتضمنها المنتوج الأصلي.

أما الخداع حسب المادة 429 المشار إليها أعلاه، فإنه يقع عندما يتم المساس بأحد العناصر الجوهرية للمنتوج والتي تكون أساس اقتنائه، بحيث لو علم المستهلك بذلك لما أقدم على إقتناء هذا المنتوج. ولعل أبرز مثال عن ذلك هو وضع علامة بيولوجي وهو في الحقيقة يحتوي مواد كميائية.

الفرع الثاني : عرض أو وضع المنتجات المغشوشة للبيع على السوق الإفتراضي

إذا رجعنا إلى المادة 431 من قانون العقوبات نجد المشرع يشدد على تجريم فعل العرض أو الوضع للبيع وإن كانت مصطلحات لمعنى واحد هو وضع المنتوج تحت يد المستهلك[1]، إلا أنه

---

[1]عرف المشرع عملية وضع المنتوج للإستهلاك في القانون رقم 09-03 المؤرخ في 25 فبراير 2009 ، المتعلق بحماية المستهلك وقمع الغش، الجريدة الرسمية عدد 13، الصادرة في 08 مارس 2009.المعدل بالقانون رقم18-09 المؤرخ في 25 جوان 2018،الجريدة رسمية عدد35 الصادر في 13جوان 2018: بأنه مجموع مراحل الإنتاج والإستيراد والتخزين والنقل والتوزيع بالجملة

يستوى في نظرنا أن يكون العرض في سوق مادي أو إفتراضي لأن العبرة في العرض ووصول المنتوج إلى المستهلك الذي يقع ضحية للغش، أما الخداع بهذا المفهوم قد يتجسد في طرح بضاعة في السوق لا تعكس ما يروج له في الموقع الخاص بالمنتج سواء كان من حيث النوع أو الكم أو حتى المصدر.

تجدر الإشارة في الأخير أن قانون حماية المستهلك وقمع الغش الجزائري[1] قيد المنتج مجموعة من الإلتزامات أولها ضمان الأمن ثم الضمان بصفة عامة وضمان وخدمة ما بعد البيع ، إلزامية مطابقة المنتوجات وإعلام المستهلك.

المبحث الثاني شروط قيام المسؤولية الجزائية للشركات التجارية عنها

تقوم مسؤولية الأشخاص الطبيعية عن جريمتي الغش والخداع بمجرد تحقق أركان الجريمتين فقط، خلفا لذلك فإنه لإقامة المسؤولية الجنائية للشركات التجارية عنها، لابد من تحقق أركان الجريمتين بالإضافة إلى الشروط والضوابط التي حددها المشرع في المادة 51 مكرر من قانون العقوبات الجزائري.

وعموما يمكن رد هذه الشروط إلى أربعة شروط أساسية، يتعلق الأول بطبيعة الشخص المعنوي الذي يسأل جنائيا، والثاني يتعلق بوجود النص الذي يجرم الشركات ، والثالث يتعلق بوجوب إرتكاب جريمة الخداع بواسطة شخص طبيعي له سلطة التعبير عن إرادة الشخص المعنوي، والرابع يتعلق بضرورة إرتكاب الجريمتين لحساب الشخص المعنوي[2].

المطلب الأول : إرتكاب جريمة الغش والخداع الإلكتروني من طرف مورد إلكتروني

حدد المشرع جملة من الشروط في نص المادة 51 مكرر من قانون العقوبات ومن بينها ضرورة إرتكاب الجريمة من طرف شخص معنوي خاضع للقانون الخاص، وأن ينص القانون على مسؤولية عن الجريمة. فهل يتصور تحقق هذين الشرطين بالنسبة لجريمة الغش والخداع الإلكتروني؟

الفرع الأول: إرتكاب جريمة الغش والخداع الإلكتروني من طرف مورد إلكتروني(شركة تجارية)

---

[1] **TH.DALMASSO**,la responsabilité pénale des personnes morales,édEFE,France, 1996,p55.

[2] راجع نصوص المواد من 09 إلى 18 من قانون حماية المستهلك وقمع الغش.

لابد لقيام المسؤولية الجزائية للشركات التجارية عن جريمة الغش والخداع أن تقوم الشركة بعرض أو تسويق منتوج معين عن طريق الإتصالات الإلكترونية، وهو ما سماه المشرع "**بالمورد**" في قانون التجارة الإلكترونية[1]، وعرفه على أنه" كل شخص طبيعي أو معنوي يقوم بتسويق أو إقتراح توفير السلع أو الخدمات عن طريق الإتصالات الإلكترونية". أو "**بالمتدخل**" في المادة 03 في قانون حماية المستهلك وقمع الغش وعرفه على أنه "كل شخص طبيعي أو معنوي يتدخل في عملية عرض المنتوجات للإستهلاك".(7)

الفرع الثاني : وجود نص التجريم (مبدأ التخصيص)

لم يتخلف المشرع الجزائري كعادته بالإقتداء بنظيره الفرنسي بأن قيد مسؤولية الشركات التجارية بمبدأ التخصيص، رغم الإنتقادات المتكررة التي تعرض لها المشرع الفرنسي. حيث يرى البعض أن مبدأ التخصيص ما هو إلا انعكاس لعدم قانعة المشرع بالإعتراف بمسؤولية الشركات وبوجودها الحقيقي، بالإضافة إلى أن هذا المبدأ سوف يسمح بإفلات العديد من الأشخاص من العقاب، نظرا لعدم إمكانية مواكبة المشرع جميع التطورات، خاصة تلك المرتبطة بالميدان الإقتصادي.

غير أنه فيما يتعلق بجريمة الغش والخداع لم يتوانى المشرع في التنصيص صراحة على مسؤولية الشركات التجارية وذلك بموجب المادة 435 مكرر من قانون العقوبات حيث جاء فيها" يكون الشخص المعنوي مسؤولا جزائيا عن الجرائم المعروفة في هذا الباب". كما يمكن إستنتاج تحقق شرط التخصيص من قانون حماية المستهلك 09-03 المعدل والمتمم عندما عرف المشرع المتدخل بأنه كل شخص طبيعي أو معنوي يتدخل في عملية عرض المنتوج للإستهلاك. ونص في المادة 70 على نفس الأفعال المحددة في المادة 431 من قانون العقوبات. أو في قانون التجارة الإلكترونية عندما عرف المورد الإلكتروني بأنه كل شخص طبيعي أو معنوي كما أشرنا أعلاه.

المطلب الثاني: إرتكاب جريمة الغش والخداع الإلكتروني من طرف شخص طبيعي له سلطة التعبير عن إرادة الشخص المعنوي الخاص ولحسابه

إن الشخص المعنوي ككيان قانوني لا يمكنه التصرف إلا بواسطة أجهزته أو ممثليه الشرعيين كما جاء في المادة 51 مكرر من قانون العقوبات. حيث يمكن تحديد ماهية الأجهزة

---

[1] القانون رقم 18-05 الصادر في 10 ماي 2018 المتعلق بالتجارة الإلكترونية، الجريدة الرسمية عدد28، الصادرة في 16 ماي 2018.

وممثلين الشرعيين للشخص المعنوي بالرجوع للقانون المنظم له ولقانونه الأساسي بصفة عامة. بالإضافة إلى ذلك لابد من إرتكاب الجريمة لحساب الشخص المعنوي لإمكانية إثارة مسؤولية هذا الأخير، فمصلحة الشخص المعنوي هي الفاصل بين مسؤولية الشخص الطبيعي والمعنوي، وعليه لابد من تحديد مفهوم أجهزة الشخص المعنوي وممثليه الشرعيين والتصرفات التي تصب في مصلحته.

الفرع الأول: إرتكاب جريمتي الغش والخداع الإلكتروني من طرف أحد أجهزة الشخص المعنوي أو ممثليه الشرعيين

أشرنا سابقا أن جريمة الغش والخداع الإلكتروني تقوم على الغش والخداع في المواد الغذائية أو الطبية الموجهة للإنسان أو للحيوان. وذلك عرض أو وضع المنتجات المغشوشة للبيع على السوق الإفتراضي والخداع في نوعها أو كميتها. ولما كان الشخص المعنوي مجرد كيان قانوني لا يمكنه التصرف إلا بواسطة الأشخاص الطبيعيين المكونين له، فإنه لا يكون مسؤولا حسب المادة 51 مكرر و435 مكرر من قانون العقوبات والمادة 70 من القانون 09-03 إلا إذا إرتكبت الجريمتين من طرف "الأجهزة والممثلين الشرعيين أو القانونيين"

البند الأول: إرتكاب جريمتي الغش والخداع الإكتروني من طرف أحد أجهزة الشركة

لم يعرف قانون العقوبات الجزائري "الجهاز[1]"**organe**"، نظرا لإختلاف أنواع وأشكال الشخص المعنوي(المورد أو المتدخل)، فيكفي الرجوع إلى القوانين المنظمة له أو لقانونه الأساسي للقول أن الجهاز يتكون من شخص طبيعي أو أكثر يخول لهم القانون أو النظام الأساسي للشخص المعنوي إدارته أو تسيير والتصرف بإسمه في حدود الغرض الذي أنشأ من أجله[2]. ومن تم يفهم من خلال هذا التعريف أن الجهاز يمكن أن يكون شخصا طبيعيا كما يمكن أن يكون مجموعة من

---

[1] نشير هنا أن الفقه قدم العديد من المصطلحات تعبيرا عن العضو، فنجد الفقيه"ميشو"يطلق على العضو " les representant direct" والفقيه هوريو "le repesentant reel"،أما عبارة ORGANE حسب قاموس لروس فهي جزء حي من الجسم يقوم بوظيفة "utile dans la vie لذلك يمكن تشبيه البنيان القانوني للشركة بجسم الإنسان.

[2] شريف سيد كامل ، المسؤولية الجنائية للأشخاص المعنوية-دراسة مقارنة-،الطبعة الأولى،دار النهضة العربية،مصر،1998،ص112.

الأشخاص، لها دور محدد حسب القانون للتصرف وتجسيد إرادة ومصلحة الشخص المعنوي، ويترتب عن الأفعال التي ترتكبها قيام المسؤولية الجنائية لهذا الأخير[1].

غير أن الملاحظ على المادة 51 مكرر من قانون العقوبات، أنها لم تحدد بصفة صريحة نوع الجهاز المقصود، خاصة إذا علمنا أن الشخص المعنوي بصفة عامة والشركات التجارية بصفة خاصة تتكون من أجهزة دائمة وأجهزة مؤقتة أجهزة للتسيير وأجهزة للمراقبة، فيرى البعض أنه من الناحية العملية أن مجلس المراقبة والجمعية العامة للمساهمين في شركات المساهمة يصعب تصور إقامة مسؤوليتها لطبيعة الوظيفة الموكلة إليهما فمجلس المراقبة يرصد لمراقبة حسن عمل وتسير الشركة عن طريق المداولات، والجمعية العامة كذلك فوظيفة كليهما هي ظرفية ومؤقتة. فحين يلقى على عاتق باقي الأجهزة مهمة التسيير اليومي للشركة بالنسبة لباقي الشركات[2].

عموما فإن الأجهزة الشرعية لشركة التضامن هي "**المدير** " الذي يمكن أن يكون شخصا واحد أو أكثر ويمكن أن يعين من بين الشركاء أومن الغير، فإذا كان تعيينه في العقد التأسيسي للشركة سميا مديرا نظاميا وإذا عين بموجب إتفاق لاحق سمي بالمدير غير نظامي، بالإضافة إلى المدير فإن الجمعية العامة للمساهمين تعتبر هي الأخر جهازا للشركة.

[1]نشير هنا إلى قرار صادر عن المحكمة العليا بتاريخ 28-204-2011 ،غرفة الجنح و المخالفات ،في الملف رقم 613327 ،قرار منشور في مجلة المحكمة العليا ،العدد 01-2011.بنقض قرار المجلس القضائي للعاصمة الذي أذان بنك سوسيتي جنرال بجنحة مخالفة التشريع و التنظيم الخاصين بالصرف وحركة رؤوس الأموال من وإلى الخارج.

[2] محمد حزيط، المسؤولية الجزائية للشركات التجارية في القانون الجزائري و القانون المقارن،دار هومه،الجزائر،2013 ،ص202.

-أشار إلى نفس الرأي كل من الفقيهين الفرنسيين "F.DESPORTS ET F LE GUNEHEC"حيث يريان كلاهما أنه من الناحية العملية فغن أجهزة التسيير وحدها قابلة لأن تجعل الشخص المعنوي مسؤولا جزائيا، أما أجهزة المراقبة فلا يترتب على أنشطتها قيام المسؤولية الجزائية للشخص المعنوي. أشار إلى ذلك :أحمد الشافعي، الإعتراف بمبدأ المسؤولية الجزائية للشخص المعنوي في القانون الجزائري، رسالة دكتوراه في القانون، كليةالحقوق، جامعة بن يوسف بن خدة،الجزائر،2011-2012،ص247.

أما الأجهزة الشرعية لشركة التوصية البسيطة فتتمثل في "**المدير**" الذي يعين من بين الشركاء المتضامنين دون الموصين وإلا إعتبر متضامنا ومسئولا عن ديون الشركة بصفة مطلق وغير محدودة، بالإضافة المدير فإن الجمعية العامة للمساهمين تعتبر جهازا كذلك[1].

فحين يتطلب لتحديد أجهزة شركة المساهمة أولا تحديد النظام الذي تتخذه الشركة، فإذا كانت تتخذ نمط التسيير عن طريق مجلس المديرين فإن أجهزتها تمثل في مجلس المديرين ورئيس مجلس المديرين والممثلين المعنيين من طرف مجلس المراقبة وأخيرا مجلس المراقبة. أما إذا كانت الشركة مسيرة وفقا لنظام مجلس الإدارة فإن أجهزة الشركة تتلخص في مجلس الإدارة ورئيس مجلس الإدارة والرئيس المدير العام والمديرين العامين عندما توكل إليهم مهمة إدارة الشركة في نفس الوقت. بالإضافة ما سبق فإن الجمعية العامة هي أخرى تعتبر جهازا في شركة المساهمة في كلا النظامين[2].

كما لا تختلف كثيرا أجهزة الشركة ذات المسؤولية المحدودة عن باقي الشركات، فالمدير يعد جهازا وإن تعددوا، وسواء عين بالعقد التأسيسي أو بموجب إتفاق لاحق من بين الشركاء أو من الغير، ويكون المدير جهازا شرعيا في الشركة ذات المسؤولية المحدودة ذات الشخص الوحيد سواء كان شريكا أو أجنبيا[3].

البند الثاني : إرتكاب جريمة الغش والخداع من طرف الممثلين الشرعيين للشركة التجارية

يذهب بعض الفقه[4] إلى التفرقة بين الممثل "***représentant***" وبين العضو "***organe***"، على إعتبار أن العضو هو الممثل القانوني أو الشرعي للشخص المعنوي. فتعبير الأعضاء يشمل الرئيس المدير العام، والمديرين ومجلس الإدارة ومجلس المراقبة والجمعية العامة للمساهمين، بينما الممثل هو

---

[1] - فتيحة يوسف، أحكام الشركات التجارية وفقا للنصوص التشريعية و المراسيم التنفيدية الحديثة،الطبعة الثانية، دار الغرب،الجزائر،2007

[2] أحمد قائد مقبل ، المسؤولية الجنائية للشخص المعنوي-دارسة مقارنة-،الطبعة الأولى، دار النهضة العربية،مصر،2005،ص121

[3] عمر سالم، المسؤولية الجنائية للأشخاص المعنوية وفقا لقانون العقوبات الفرنسي الجديد،الطبعة الأولى،،دار النهضة العربية،مصر،1995،ص49.

[4] محمد أحمد المحاسنة، المسؤولية الجزائية للشخص المعنوي في حالة إنتفاء الصفة التمثيلية للعضو مرتكب الجريمة-دراسة مقارنة، مجلة دراسات علوم الشريعة والقانون،العدد01،المجلد42،سنة2005،تصدر عن الجامعة الإردنية،الأردن،ص138.

الشخص الطبيعي صاحب السلطة القانونية أو الإتفاقية للتصرف بإسم الشخص المعنوي، فقد يكون المدير العام بمفرده أو المدير الإداري أو رئيس مجلس الإدارة[1].

غير أنه في حقيقة الأمر يعتبر الجهاز والممثل وجهان لعملة واحدة، ففي بعض الشركات يختلط مفهوم الجهاز مع الممثل لأن الجهاز يكون مسئولا عن تمثيل الشركة، فحين يظهر جليا في بعض الشركات الأخرى الفرق بينهما كما هو الحال بالنسبة للمتصرف المؤقت الذي يعين لمدة ظرفية فقط أو كحال المسير الأجنبي الذي يعين بموجب إتفاق لاحق للعقد التأسيسي[2].

فقد عرف المشرع الجزائري الممثل الشرعي في الفقرة 02 من المادة 52 مكرر02 من قانون الإجراءات الجزائية بأنه«هو الشخص الطبيعي الذي يخوله القانون أو القانون الأساسي للشخص المعنوي تفويضا لتمثيله». وبالتالي فإن ممثل شركة التضامن وشركة التوصية البسيطة هو "المدير" ،أما ممثل شركة المساهمة فهو رئيس المدير العام والمدير العام أو رئيس مجلس الإدارة أو رئيس مجلس المديرين،وأعضاء مجلس المديرين المفوضين من قبل مجلس المراقبة .وجميع الأشخاص الطبيعية المخولة لتمثيل الشركة بموجب القانون الأساسي أو إتفاق لاحق .

ما نخلص في الأخير أن المشرع ضيق من مفهوم "**الممثل**" وقيده بشرط الشرعية، وبات يتطلب لإقامة مسؤولية الشخص المعنوي عن جريمتي الغش الضريبي وتبييض الأموال إرتكاب السلوك المادي المكون للجريمتين من طرف الممثل الشرعي أي الذي يكتسب سلطاته من القانون أو القانون الأساسي للشركة، ويقصي بذلك جميع الأشخاص الحائزين على تفويض أو توكيل من قبل أحد الأجهزة أو الممثلين الشرعيين.

الفرع الثاني إرتكاب جريمة الغش والخداع لحساب الشركات التجارية

بالإضافة إلى ضرورة إرتكاب جريمة الغش والخداع الإلكتروني من طرف أحد أعضاء أو ممثلي الشخص المعنوي الشرعيين، يجب أن ترتكب لحسابه. وهو ما إعتباره المشرع شرطا أساسيا لقيام مسؤولية الشركات. فالقاضي الجزائي ملزم بإثبات إرتكاب الجريمة من طرف أحد أعضاء أو ممثلي الشخص المعنوي الشرعيين، وأنهم إرتكبوا الجريمة لحسابه، غير أن الملاحظ على

[1] محمد أبو العلا عقيدة،الإتجاهات الحديثة في قانون العقوبات الفرنسي الجديد،دار الفكر العربي،مصر،1997،ص55.

[2] محمد أحمد المحاسنه، المسؤولية الجزائية للشخص المعنوي في حالة إنتفاء الصفة التمثيلية للعضو مرتكب الجريمة-دراسة مقارنة،مجلة دراسات علوم الشريعة والقانون،العدد01،المجلد42،سنة2005،تصدر عن الجامعة الإردنية،الأردن ،ص138.

المادة 51 من قانون العقوبات السالفة الذكر لم توضح بشكل دقيق معنى عبارة "لحساب" أو *pour leur compte*" مما سوف يفسح المجال أمام القاضي لإعمال سلطته التقديرية في تحديد الأفعال التي يمكن تأويلها لحساب الشخص المعنوي.أي لا فائدة من التنصيص على هذا الشرط لأن جميع الجرائم التي ترتكب من قبل الشخص المعنوي خاصة منها الإقتصادية تصب في مصلحته .

حيث يرى بعض الفقه[1]أن "**عبارة لحساب الشخص المعنوي** " تقتضي أن تكون الجريمة قد إرتكبت بهدف تحقيق مصلحة له، كتحقيق الربح أو تجنب إلحاق ضرر به ويستوي أن تكون هذه المصلحة مادية أو معنوية، مباشرة أو غير مباشرة، محققة أو احتمالية، أي يكفي أن تكون الأفعال الإجرامية قد ارتكبت بهدف ضمان تنظيم أو حسن سير أعمال الشخص المعنوي أو تحقيق أغراضه.

خاتمة:

نخلص في الأخير للقول أن المشرع لم ساوى بين الغش والخداع العادي وذلك الواقع في المجال الإفتراضي، فيشترط أن يقع الغش على مواد غذائية أو طبية تكون موجهة للإنسان أو الحيوان وأن يتم عرضها للبيع، أما الخداع فيكون عندما يقع مساس بالصفات الجوهرية للمنتوج وخصائصه. فيكون بذلك آخر مرحلة لإتمام الجريمة. ومع ذلك لا تكون الشركة المنتجة للسلع المغشوشة مسؤولة على جريمة الغش و الخداع إلا ثبت أن الغش وقع من طرف أحد أجهزتها أو ممثليها ، ووقع لحسابها. أما عن مبدأ التخصيص فأحسن ما فعل المشرع عندما شرع النص المجرم لأنه الأشخاص المعنوية عادة ما تستعمل كغطاء للتهرب من العقاب.

في الأخير ما تجدر الإشارة إليه أن جريمة الغش والخداع الإلكتروني من أكثر الجرائم إنتشارا لضعف الحماية الإلكترونية، ولإهمال الدولة لهذا السوق الخصب. وعليه نناشد المشرع:

-باستحداث آليات الدفع الإلكتروني وتنظيم السوق الإلكترونية وتشجيع التعامل داخلها لما لها من منافع اقتصادية.

-وضع برامج إلكترونية للتدقيق في حقيقة السلع المعروضة، وتتبع مصدرها.

-إنشاء برامج تكوينية لأعوان الرقابة للسماح بممارسة وظائفهم الرقابية على المنتجات المعروضة على الإنترنيت.

---

[1] محمد نصر محمد القطري، المسؤولية للشخص المعنوي-دراسة مقارنة-، مجلة العلوم الإنسانية والإدارية،ع20،05،..،صادرة عن جامعة المجمعة،الأردن،ص45

خصوصية العقاب في الجريمة المعلوماتية

The privacy of punishment in information crime

د. صورية بورباية أستاذة محاضرة أ
جامعة طاهري محمد- بشار- الجزائر

مقدمة

العقاب عن الجرائم المعلوماتية هو الجزاء القانوني الرادع لكل من يشارك أو يقوم بالاعتداء على المعلومات وعناصر نظم المعالجة الآلية للمعطيات، و كذا ضمان الأمن واسترجاع الحقوق في حالة الاعتداء عليها.

وهذا ما أكدته اتفاقية بودابست بشأن الجرائم الالكترونية، وعلى ضرورة تكريس عقوبات فعالة ملائمة ورادعة تتناسب و خطورة الأفعال الواقعة على نظم المعالجة الآلية للمعطيات.

حيث أشارت هذه الاتفاقية على ضرورة أن يكون كل فعل مجرم تم النص عليه فيها مستحق لجزاءات عقابية والتي يجب أن تكون فعالة وملائمة ورادعة، وذلك للحيلولة دون حدوث نتائج خطيرة[1]، وهذا ما وضحته بموجب المادة 13 تحت عنوان الجزاءات والإجراءات.

و هذا التأكيد نابع من خطورة هذه الجرائم و خسائرها على الاقتصاد الوطني، وانتشار الوعي بهذا الأمر، و أنا صعوبة التصدي لهذا الخطر والتهديد نابع من صفة بعض الأشخاص قد يطلق عليهم تسمية" المتطفلين الأذكياء"[2] والذين يمكن تسخيرهم من قبل الجهات والحكومات للحصول على ما هو أثمن وأخطر، سواء من أجل المنافسة أومن أجل امتلاك مركز القوة، فمن يمتلك المعلومة يمتلك القوة .

كما أن هذه الأخطار لا ترتكب من قبل أشخاص معينين، بل من قبل جميع الأشخاص والفئات والطبقات، وذلك نتيجة انتشار التكنولوجيا وتبسيط وسائل الاتصال، وانتشار

---

[1]- د. **هلالي عبد اللاه أحمد**، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية، على ضوء إتفاقية بودابست الموقعة في 23 نوفمبر 2001، الطبعة الأولى، دار النهضة العربية، القاهرة- مصر، 2003، ص 155،154.

[2]- لتفاصيل أكثر لدى: د.**دلال صادق الجواد** ود.**حميد ناصر الفتال**، أمن المعلومات، دار اليازوري، عمان- الأردن، 2008، ص 141

الانترنت[1]، ضف إلى ذلك دخول الجزائر في السنوات الأخيرة تكنولوجيا الجيل الثالث و الرابع، وعلى الرغم من التأخر التكنولوجي في الجزائر وضآلة نتائج التطور مقارنة مع الدول العالم، إلا أنها ليست بمعزل عن الأخطار المعلوماتية التي أصبحت تهدد امن أكبر دول العالم.

و من اجل ذلك سارع المشرع الجزائري إلى إدخال تعديلات على قانون العقوبات في الفصل الثالث المتضمن الجنايات والجنح ضد الأموال، وإضافة قسم سابع مكرر متعلق بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم 04_15 وتعديله من جديد في 2006 بموجب القانون رقم 06-23[2] حيث شدد فيه عقوبة الغرامة دون المساس بالنصوص التجريمية الواردة بشان المساس بأنظمة المعالجة الآلية.

و نفس الأمر بالنسبة للمشرع الفرنسي، وبناء على الوضع القائم قام بتعديل قانون العقوبات وفي كل مرة يشدد فيها العقاب على الجرائم المتعلقة بالمعالجة الآلية للمعطيات، من تلك التعديلات نجد تعديل سنة 2004 بموجب القانون 2004-575 المؤرخ في 21 جوان والمتعلق بالثقة في الاقتصاد الرقمي[3] الذي جاء فيه تشديد عقوبة الحبس والغرامة المقررة لهذه الجرائم وذلك بموجب المادة 45 الفصل الثاني منه بعنوان مكافحة جرائم الفضاء المعلوماتي.

1- أ. **رشيدة بوكر**، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن،ط1، منشورات حلبي الحقوقية، بيروت- لبنان، 2012، ص 315.

2- القانون رقم 23/06 المعدل لقانون العقوبات المؤرخ في 20 ديسمبر 2006

3 -**Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,** JORF n°0143 du 22 juin 2004 page 11168 texte n° 2. Chapitre II : Lutte contre la cybercriminalité Art 45 :

Art 45 ;

I. - L'article 323-1 du code pénal est ainsi modifié :

1° Au premier alinéa, les mots : « d'un an » sont remplacés par les mots : « deux ans » et la somme : « 15 000 EUR » est remplacée par la somme : « 30 000 EUR » ;

2° Au second alinéa, les mots : « deux ans » sont remplacés par les mots : « trois ans » et la somme : « 30 000 EUR » est remplacée par la somme : « 45 000 EUR ».

II. - A l'article 323-2 du même code, les mots : « trois ans » sont remplacés par les mots : « cinq ans » et la somme : « 45 000 EUR » est remplacée par la somme : « 75 000

حيث يثبت تدخل المشرع وتشديده العقاب على هذه الجرائم إدراكا منه بخطورة الوضع وضرورة وجود عقاب رادع.

و السؤال الذي يمكن طرحه في هذا المقام هو هل العقوبات الواردة بهذه النصوص هي كافية لردع هذه الأفعال أو للحد و الوقاية من جرائم تقنية المعلومات؟ آم لا بد من احتياطات واستراتيجيات أخرى؟ نحاول معرفة ذلك من خلال منهجية تحليلية مقارنة لنصوص التشريع الجزائري و الفرنسي و ما جاء في الاتفاقيات الدولية وفقا للخطوات والعناصر الآتية:

المطلب الأول: مضمون العقاب في مجال الجريمة المعلوماتية

إن العقاب الجنائي رادع سواء بالنسبة للأشخاص الطبيعية بفرض عقوبة الحبس والغرامة، وكذا بالنسبة للأشخاص المعنوية تنشأ مسؤوليتها وتكون خاضعة لجزاءات نوضحها بحسب ما جاء في التشريع الجزائري و التشريعات المقارنة كما يأتي:

الفرع الأول: العقوبات بالنسبة للأشخاص الطبيعية

أوضحت النصوص القانونية سواء في التشريع الجزائري أوفي التشريعات المقارنة العقوبات الأصلية المقررة لمختلف الجرائم المعلوماتية، وإضافة إلى ذلك عقوبات تكميلية.

البند الأول: العقوبات الأصلية

العقوبات الأصلية هي كل عقوبة لا توقع إلا إذا نطق بها القاضي وحدد نوعيتها ومقدارها و هي السجن أو الحبس أو الغرامة المالية التي تكون كافية بذاتها لتحقيق معنى الجزاء وهي العقاب الأساسي للجريمة[1].

يحدد القانون لكل جريمة عقوبة، وتشدد العقوبة إذا اقترنت بظرف من ظروف التشديد المنصوص عليها، لذلك سوف أحاول توضيح العقوبات التي تخضع لها كل جريمة من الجرائم التي نص عليها التشريع العقابي الجزائري،مقارنة مع التشريع العقابي الفرنسي لتوضيح أكثر.

و هي تشمل العقاب على الجرائم الآتية:

EUR ».

III. - A l'article 323-3 du même code, les mots : « trois ans » sont remplacés par les mots : « cinq ans » et la somme : « 45 000 EUR » est remplacée par la somme : « 75 000 EUR ».

[1]- **راضية مشري** ، الحماية الجزائية للمصنفات الرقمية في ظل قانون حق المؤلف، مجلة التواصل لكلية الحقوق، جامعة 08 ماي 45، قالمة، عدد 34، جوان 2013، ص 144.

اولا: عقوبة جرائم المساس بأنظمة المعالجة الألية للمعطيات

و هي تتضمن الجرائم الاتية:

1: عقوبات جريمة الدخول أو البقاء غير المصرح بهما:

تختلف العقوبة في هذه الجريمة وبحسب ما ترتب أولم يترتب عن الدخول أو البقاء أضرار مست المعلومات وأنظمة المعالجة الآلية في التشريع الجزائري والتشريعات المقارنة محل الدراسة وفقا لما يلي:

أ- **العقوبة في التشريع الجزائري:** حددتها المادة 394 مكرر من قانون العقوبات و المعدلة بموجب القانون 06-23 الذي شدد عقوبة الغرامة في صورتها البسيطة والمشددة، و عليه تكون العقوبة الحبس من ثلاثة(03) أشهر إلى سنة و الغرامة من خمسون ألف(50000) إلى مائتي ألف (200000) دينار جزائري في حالة الدخول أو البقاء غير المصرح بها، و لم ينشأ عن ذلك أي ضرر أو إفساد أو تعطيل للنظام المعلوماتي المخترق أو للمعلومات المتضمنة فيه، و ذلك بعد ما كانت عقوبة الغرامة قبل التعديل لقانون العقوبات سنة 2006 تتراوح بين خمسون ألف(50000) إلى مائة ألف (100000) دينار جزائري كحد أقصى ، ولا شك أن هدف المشرع من وراء تشديد و مضاعفة الحد الأقصى للغرامة هو مكافحة ومحاولة الحد من انتشار جرائم الإختراق المعلوماتي خاصة و الجريمة المعلوماتية عامة، لاسيما إذا تم اختراق نظام يحتوي على معلومات سرية أو تتعلق بأمن الدولة و مؤسساتها[1] مما يشكل خطورة على الأشخاص و على الدولة الجزائرية التي تتوجه مؤخرا نحو إرساء حكومة إلكترونية[2] تقيدا بمبدأ العصرنة و التوجه نحو التكنولوجيا الرقمية و الانفتاح عليها.

أما إذا ترتب على فعل الدخول أو البقاء أضرار تمس المعلومات أو النظام فإن المادة 394مكرر من قانون العقوبات المعدل و في فقرتيها الثانية و الثالثة تنص على أنه"...تضاعف العقوبة إذا

---

[1]- و هذا ما أكد عليه المشرع الجزائري و أخده بعين الاعتبار، عندما لم يقصر الحماية على المعلومات بمختلف أنواعها و بغض النظر عن الجهات التي تنتمي إليها،بتشديده للعقوبة إذا كانت المعلومات التي تم الاعتداء عليها تتعلق بالدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام و ذلك بموجب المادة 394 مكرر3 من قانون العقوبات المعدل.

[2]- يظهر توجه الجزائر نحو تفعيل الحكومة الالكترونية من خلال إصدار تشريعات للتواصل في المسائل الإدارية و غيرها مع المواطنين من خلال القانون رقم 15-03 مؤرخ في أوّل فبراير سنة 2015 يتعلق بعصرنة العدالة ،و القانون رقم 15-04 مؤرخ في أوّل فبراير سنة 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني، ج.ر عدد 06 بتاريخ السادس من فبراير 2015، ص 4-6.

ترتب على حذف أو تغيير لمعطيات المنظومة، و إذا ترتب على الأفعال المذكورة أعلاه تخريب إشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50000 دج إلى 300000 دج".

و ما هو ملاحظ في هذه الصورة لجريمة الدخول و البقاء المرتب لنتيجة، أن جعل المشرع الضرر الناتج عن ذلك الفعل ظرفا لتشديد العقوبة في حالتين اثنتين و هما:

* **إذا ترتب عن الدخول أو البقاء حذف أو تغيير لمعلومات المنظومة:** فإن العقوبة تضاعف عن تلك المقررة لعقوبة الدخول أو البقاء المجرد ليصبح الحبس في حده الأدنى (06) ستة أشهر و في حده الأقصى (02) سنتين، والغرامة لتتراوح بين (100000) مائة ألف دينار جزائري إلى (400000) أربعمائة ألف دينار جزائري.

* **إذا ترتب عن فعل الدخول أو البقاء تخريب نظام اشتغال المنظومة:** و في هذه الحالة تكون عقوبة الحبس من (06) ستة أشهر إلى (02) سنتين، أما الغرامة فتكون بين (50000) دينار جزائري إلى احدها الأقصى (300000) ثلاثمائة ألف دينار جزائري.

و الملاحظ أن المشرع لم يعطي للقاضي الفاصل في المنازعة الحكم بإحدى العقوبتين الحبس أو الغرامة باستعمال حرف "واو" الربط بدلا من " أو" الاختيارية دون ترك المجال للسلطة التقديرية للقاضي في إمكانية الجمع من عدمه، و يكون المشرع الجزائري في ذلك قد جانب الصواب، لأنه يمكن للقاضي الحكم بإحدى العقوبتين مما قد يجعل العقاب أقل ردعا، و بإمكان القاضي أن يحكم بجعل الحبس أو الغرامة أو كلاهما معا موقوفة النفاذ طبقا لنص المادة 592 قانون إجراءات جزائية[1]، فضلا عن إمكانية تطبيق عقوبة العمل للنفع العام بدلا من الحبس طبقا للمادة 05 مكررا1 من قانون العقوبات، و يكون للقاضي سلطة تقديرية في الحكم بالعقوبات بين الحد الأدنى والحد الأقصى بحسب ما تتطلبه كل حالة الاختراق.

ب- **العقوبة في التشريع الفرنسي:** حدد المشرع الفرنسي عقوبات مختلفة و عدلها في كل مرة بتشديدها بداية من أول قانون لسنة 1988 المتعلق بالغش المعلوماتي و إدخاله في قانون العقوبات سنة

---

[1]- المادة 592 من الأمر رقم المتضمن قانون الإجراءات الجزائية الجزائري تقضي:" يجوز للمجالس القضائية و للمحاكم، في حالة الحكم بالحبس أو غرامة إذا لم يكن المحكوم عليه قد سبق الحكم عليه بالحبس لجناية أو جنحة من جرائم القانون العام، أن تأمر بحكم مسبب بالإيقاف الكلي أو الجزئي لتنفيذ العقوبة الأصلية" معدلة بموجب القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004، ج.ر عدد 71، ص 06 .

1992 وبدأ العمل به بداية من 1994[1]، وكذا التعديل الذي جاء في 2004 و2012، و العقاب عليها في صورتها البسيطة والمشددة.

فكانت عقوبة الدخول أو البقاء غير المشروع في صورتها البسيطة في أول قانون للغش المعلوماتي رقم 88-19 تقدر بـ (02) شهرين حبس إلى (01) سنة أو بغرامة من (2000) ألفين فرك فرنسي إلى (50000) خمسين ألف فرك فرنسي[2]، فكان الحد الأدنى و الأقصى منخفضا مع ترك السلطة التقديرية للقاضي في تقدير عقوبة ما بين الحدين مع حريته في الحكم بإحدى العقوبتين فقط.

ليأتي المشرع الفرنسي بقانون العقوبات الجديد سنة 1994 و يجعل عقوبة هذه الجرائم في حد واحد سواء كانت الحبس لمدة (01) سنة و بغرامة (15000) خمسة عشر ألف يورو ليسلب القاضي سلطته التقديرية في التحرك بالعقوبة[3].

و حالات أخرى و لأن جرائم المعالجة الآلية للمعطيات في انتشار و تطور مستمر تبعا لتطور التقنية الرقمية، و كذا لنمو و ازدياد الخسائر الناجمة عنها خاصة أن التقارير الأخيرة توضح تأثر فرنسا من ضمن الدول الأوروبية بهته الجرائم، و كذا قيامها بكل الإجراءات و التدابير لدراسة واقع الجريمة الإلكترونية و لمكافحة جرائم الانترنت لحماية شعبها من هذا الخطر المتلون و غير المحدود، إضافة إلى تشجيعها القيام بحملات تحسيسية و توعية من قبل مهنيين و متخصصين في هذا المجال،

---

[1] - **Loi n° 92-683 du 22 juillet 1992**, portant réforme du code pénal, texte origine au 01 mars 1994.

[2] -**Art** 462-2 du A.C.P.F dispose que ; « quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de deux mois à un an et d'une amende de 2000 f à 50000 f ou de l'une de ces deux peines… »**Loi n°88-19** du 05 janvier 1988 relative à **la fraude informatique**, JORF du 06 janvier 1988, P 231.Sur le site ; www.legifrance.gouv.fr

[3] -**Art** 323-1 ; « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 100 000 f d'amende… » **Loi n° 92-683** du 22 juillet 1992, portant réforme **du code pénal**, texte origine au 01 mars 1994.

وضع برامج و خطط إستراتيجية و من ذلك تقديم تقرير حول" حماية مستخدمي الانترنت"[1] الذي قام به فريق عمل وزاري تحت إشراف مارك روبرت النائب العام لمحكمة استئناف ريوم.

و الملاحظ أن المشرع الفرنسي لم يدخر أي جهد في مكافحته لجرائم أنظمة المعالجة الآلية في كل فرصة تسمح بالتعديل، فقد بدأ مبكرا في مواجهته لهذه الجرائم، و لم يتأخر[2]عن أي إجراء تعديلي كلما تطلب الأمر ذلك.

و قام المشرع الفرنسي مرة أخرى بتشديد العقوبة، و ذلك بموجب المادة (45) من الفصل الثاني من القانون رقم 2004-575 المتعلق بالثقة في الاقتصاد الرقمي لتصبح العقوبة ضعف عما كانت عليه: الحبس (02) سنتين و الغرامة (30000) ثلاثون ألف يورو.

أما عقوبة الدخول أو البقاء غير المصرح به و في صورته المشددة، حيث جعل المشرع ما يترتب عن الدخول أو البقاء بدون قصد من أضرار كظرف مشدد، فكانت في قانون الغش المعلوماتي لسنة 1988 محدد ب الحبس لمدة من (02) شهرين إلى (02) سنتين و بغرامة من (10000) عشرة ألاف فرك فرنسي إلى (100000) مائة ألف فرك فرنسي و ذلك في حالة ترتب عن الدخول أو البقاء حذف أو تعديل للبياناتاو تعطيل النظام[3].

و كذا في قانون العقوبات الجديد لسنة 1994 ليحتفظ بالحد الأقصى لعقوبة الحبس و رفع الغرامة إلى (30000) ثلاثون ألف يورو، أما قانون العقوبات لسنة 2004 كذلك زاد من عقوبة الحبس إلى (03) ثلاثة سنوات و الغرامة لتصبح (45000) خمسة و أربعون ألف يورو[4].

---

[1] -**Remise du Rapport** « Protéger les Internautes » remettre par **Marc Robert**, Procureur général prées la cour d'appel de Riom, le rapport du group de travail interministériel sur la lutte contre la cybercriminalité, communiqué de presse, N° 185, Paris, le 30 juin 2014,sur le site ; www.presse.justice.gouv.fr

[2] - **رشيدة بوكر**، مرجع سابق، ص 319.

[3] -**Art** 462-2/2 ; « Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de deux mois à deux ans et l'amende de 10000 F à 100000 F » **la loi n° 88-19** précédente.

[4] - **Art** 323-1 alinéa 2, « Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce

ليأتي المشرع الفرنسي في سنة 2012 بفقرة جديدة من نفس المادة، و يتفرد بها على غرار المشرع الجزائري و غيره من المشرعين، و يعاقب بعقوبة أشد إذا كان الدخول أو البقاء سواء في صورته البسيطة أو المشددة يرتكب على نظام معالجة آلية للبيانات الشخصية التي تنفذها الدولة[1].

2:عقوبة جريمة الإتلاف المعلوماتي او تخريب منظومة معلوماتية

أ- **في التشريع الجزائري:** اخضع المشرع الجزائري لمن تعمد منذ البداية الإضرار بمعلومات المتضمنة في نظم المعالجة الآلية او تخريب المنظومة في ذاتها لعقوبة أشد عن من دخل أو بقي بدون تصريح وترتب عن ذلك ضرر وفقا للمادة 394 مكرر 1، و لا شك أن المشرع قد شدد العقوبة في هذه الصورة عن العقوبة في الصورة الأولى لجريمة الاختراق المعلوماتي و ذلك راجع إلى توفر عنصر القصد منذ بداية ارتكاب فعل الإتلاف، فحددت العقوبة بـ (06) ستة أشهر حبس إلى (03) ثلاثة سنوات و غرامة من (500000) خمسمائة ألف إلى (2.000.000) اثنان مليون دينار جزائري لكل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش، ولم ينص على إتلاف أو تخريب نظام اشتغال منظومة المعالجة الآلية للمعطيات مكتفيا بنص المادة 394 مكرر عقوبات، إن كان إدخال معلومات فيها مثل بعض الفيروسات قد يترتب عنه تعطيل اشتغالها.

ب- **في التشريع الفرنسي:** كذلك المشرع الفرنسي نص على عقوبات إتلاف المعطيات والمعلومات المتضمنة في أنظمة المعالجة الآلية، وعلى إتلاف أو تعطيل تلك الأنظمة بموجب المادتين462-3 و 462-4 من القانون 88-19 فكانت عقوبة إتلاف أو تعطيل نظام للمعالجة الآلية للمعلومات

---

système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende » **Du code pénal français** modifié par la **loi n° 2004-575** du juin 2004 pour **la confiance dans l'économie numérique**, art 45, JORF n°0143 du 22 juin 2004, P11168, texte n°02.

[1]- **Art** 323-1 alinéa 3 **du code pénal** ; « Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende » Modifié par **LOI n°2012410** du 27 mars 2012 art 9,

هي الحبس من (03) ثلاثة أشهر إلى (03) ثلاثة سنوات و غرامة (10000) عشرة ألاف فرك إلى (100000) مائة ألف فرك فرنسي أو بإحدى العقوبتين[1].

و عقوبة إتلاف معلومات متضمنة في نظام معلوماتي هي بالنسبة للحبس نفس عقوبة تعطيل النظام الحبس من (03) ثلاثة أشهر إلى (03) ثلاثة سنوات و الغرامة اقل منها مقارنتا بسابقتها بالنسبة لحدها الأدنى و الضعف خمس مرات بالنسبة لحدها الأقصى و هي (2000) ألفين فرك إلى (500000) خمسمائة ألف فرك فرنسي أو بإحدى هاتين العقوبتين[2] .

و بعد تعديله لقانون العقوبات الجديد الذي أصبح ساريا بدايتا من مارس 1994، جعل العقوبات في حدها الأقصى فقط و هي واحدة سواء بالنسبة لإتلاف المعلومات أو إتلاف النظام و تعطيله ، بأن أصبحت عقوبة الحبس (03) ثلاثة سنوات و بغرامة (45000) خمس و أربعون ألف يورو دون أن تكون للقاضي سلطة تقديرية بين العقوبتين و ذلك بموجب المادتين 232 -2 و323-3 عقوبات فرنسي المعدل والمتمم.

ليعود المشرع الفرنسي من جديد و يستجيب للمستجدات بتعديله لهته المواد بموجب القانون رقم 2004-575 و يرفع العقوبات السابقة بالنسبة لجريمة الإتلاف سواء بالنسبة للمعطيات أو البيانات او بالنسبة لتشغيل النظام بأن يعاقب على ذلك بالحبس لمدة (05) خمس سنوات و غرامة (75000) خمس و سبعون ألف يورو.

---

[1] -**Art 462-3** ; « quiconque aura intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 10 000 F à 100 000 F ou de l'une de ces deux peines »**. Loi n°88-19** précédente.

[2] - **Art 462-4** ; « quiconque aura intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 2000 F à 500000 F ou de l'une de ces deux peines » **Loi n°88 -19**

و لقد فسر تقارب العقوبتين بالنسبة لصور الإتلاف المعلوماتي من قبل الجمعية الوطنية الفرنسية بالتقارب الكبير بين الجريمتين، و يتعذر التمييز بينهما في بعض الأحيان، كما فسر أن فعل إعاقة النظام يكون نتيجة إدخال معلومات و هي صورة من صور إتلاف أو التلاعب بالمعلومات[1].

و في 2012[2] و مؤخرا في 2014 ليعدل المادة 233-3[3] و يضيف المشرع الفرنسي في المادتين323-2 و 323-3 زيادة عقوبة الحبس (07) سبع سنوات و غرامة (100000) مائة ألف يورو إذا وقع الإتلاف المعلوماتي أو جريمة التلاعب المعلوماتي على نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة.

3: عقوبة جريمة التعامل في معلومات غير مشروعة

هذه الجريمة نص عليها كل من التشريع الجزائري

أ- **التشريع الجزائري:** عاقب على هذه الجريمة بالحبس من(02) شهرين إلى (03) ثلاثة سنوات و بغرامة من (1.000.000) مليون دينار إلى (5.000.000)خمسة ملايين دينار

---

[1]- **محمد خليفة**، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة الإسكندرية 2007 ، ص192.

[2] -**Art 323-2 alinéa 2** du **C.P.F**; « Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende » **Art 323-3 alinéa 2** ; « Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende » **Loi n° 2012-410** du 27 mars 2012 précédente.

[3] -**Art 323-3** ; « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende » modifie par **LOI n°2014-1353** du 13 novembre 2014 **renforçant les dispositions relatives à la lute contre le terrorisme**, art. 16, JOPF n° 0263 du 14 novembre 2014, P 19162, texte n°5.

جزائري و ذلك بموجب المادة 394 مكرر 2 الفقرة 1 عقوبات المعدل و المتمم و يلاحظ أن عقوبة هذه الجريمة مقارنتا مع الجريمتين السابقتين، أن المشرع خفض من الحد الأدنى لعقوبة الحبس بداية من شهرين و رفع من عقوبة الغرامة كحد أقصى هو خمسة ملايين دينار جزائري، و قد يرجع السبب في ذلك إلى أن الأضرار المترتبة عن جريمة التعامل بمعلومات غير مشروعة قد تفوق بكثير الأضرار المترتبة عن الجريمة الأولى و الثانية.

ب- **التشريع الفرنسي:** يعاقب عليها المشرع الفرنسي بموجب المادة 323-3-1 عقوبات المضافة بموجب القانون 2004-575 المتعلق بالثقة في الاقتصاد الرقمي، و المعدلة بموجب القانون رقم 2013-1168 و أن العقاب على هذه الجريمة يكون بنفس العقوبة المقررة للجريمة نفسها أي العقوبة المقررة لجريمة الدخول أو البقاء غير المصرح بهما أو جريمة إتلاف المعلومات، أو نظم المعالجة الآلية التي يمكن أن تؤدي البرامج و الأجهزة والوسائل المتعامل فيها إلى ارتكابها أو بعقوبة أشد[1].

اعتبر المشرع الفرنسي و هو ما لم يقم به المشرع الجزائري، أن هذه الجريمة من الأعمال التحضيرية لجريمة أخرى قد تكون للتحضير للقيام بدخول غير مصرح أو إتلاف معلوماتي لذلك عاقب بنفس عقوبة الجريمة المحضر لها، أو بعقوبة أشد و حسن فعل المشرع الفرنسي.

البند الثاني: العقوبات التكميلية

نص القانون على عقوبات تكميلية يحكم بها إلى جانب العقوبات الأصلية و المتمثلة في المصادرة و الغلق و هو ما سيتم شرحه كما يأتي:

أولا: المصادرة

[1] -Art 323-3-1 du C.P.F « Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée » Modifié par Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, JORF n°0294 du 19 décembre 2013 page 20570 texte n° 1

يتم مصادرة الأشياء التي يتم حيازتها واستخدامها لأغراض إجرامية حيث تشمل الأجهزة و البرامج و الوسائل المستخدمة في إرتكاب جريمة من الجرائم الماسة بأنظمة المعالجة الآلية، و لقد نص المشرع الجزائري في المادة 394 مكرر 6 على أنه : "مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة و البرامج والوسائل المستخدمة"

وكذلك المشرع الفرنسي نص على عقوبة مصادرة الأشياء التي استخدمت في ارتكاب جرائم المعالجة الآلية بموجب المادة 323-5 الفقرة الثالثة من قانون العقوبات الفرنسي[1].

ثانيا: الغلق

إلى جانب عقوبة المصادرة نص المشرع على عقوبات تكميلية أخرى وهي الغلق، ويقصد بها وفقا لما جاء في المادة 394 مكرر 6: "إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على ذلك إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها".

غير أن المشرع لم يحدد مدة الغلق و هل يكون الغلق نهائيا؟

و بالنسبة للمشرع الفرنسي نص عليها في المادة 323-5 الفقرة 4 على "الغلق لمدة (5) خمس سنوات أو أكثر للمؤسسات أو لواحد أو أكثر من فروع المشروع الذي أستخدم في ارتكاب الجريمة" و إضافة إلى عقوبة الغلق والمصادرة، نص المشرع الفرنسي على عقوبات أخرى تكميلية وجوبية وبحسب طبيعة كل جريمة وظروفها بموجب نفس المادة[2].

---

[1] -Art 323-5 alinéa 3 du C.P.F : « Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ; »

[2] -Art 323-5 du C.P.F « Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;

2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

الفرع الثاني: العقوبات بالنسبة للأشخاص المعنوية

كرس القانون مبدأ المسئولية الجزائية للشخص المعنوي، وقرر له عقوبات، حيث أقر المشرع الجزائري بذلك بموجب المادة 51 مكرر من قانون العقوبات واستثنى الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام كونها هي الحامية للمجتمع وتحافظ على أمن وسلامة الأشخاص.

و يكون الشخص المعنوي مسئولا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون على ، و نص المشرع في المادة 394 مكرر 4 على الحد الأقصى للعقوبة المقررة للشخص المعنوي وهي غرامة تعادل (05) خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

أما إذا ارتكبت إحدى الجرائم السابقة من شخص معنوي على إحدى الجهات العامة أو إستهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد حسب المادة 394 مكرر3 عقوبات، وبالتالي تضاعف العقوبة مرتين إذا كانت من شخص معنوي ضد شخص معنوي أو أحد الجهات العامة، و بذلك يكون مجموع الغرامة 10 مرات أضعاف الغرامة المقررة للشخص الطبيعي.

أما بخصوص المشرع الفرنسي، نجده قد ضاعف الغرامة إلى 05 أضعاف ما يفرض على الشخص الطبيعي بموجب الفقرة الأولى من المادة 323-6 والتي أحالت في تحديد العقوبات و كيفيتها إلى مواد أخرى من قانون العقوبات[1].

4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés;

5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;

6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35

[1] -Art 323-6 du C.P.F Modifié par LOI n°2009-526 du 12 mai 2009 - art. 124 : «

المطلب الثاني: نطاق العقوبة في مجال الجريمة المعلوماتية

قد يتطلب ارتكاب بعض الجرائم البدء في القيام بنشاط إجرامي يؤدي مباشرة إلى إرتكاب الجريمة، أو القيام ببعض الأعمال لتنفيذ تلك الجريمة، و على ذلك لم تكتفي بعض التشريعات على تجريم أفعال قد تمس امن المعلومات المعالجة أو أمن أنظمتها المعلوماتية بل عاقبت حتى على الاتفاق السابق على تلك الجرائم أو الشروع فيها، و عملا بالأحكام العامة فإن الأفعال التي تسبق البدء في التنفيذ فلا عقاب عليها، و لكن نظرا لخطورة هذه الجرائم قد يخرج المشرع عن ذلك الأصل رغبتا منه لزرع الرهبة و الردع في نفوس مجرمي هذا الشكل من الإجرام، و كذا الحيلولة دون ارتكاب تلك الجرائم، و بغرض تقرير نوع من الحماية الوقائية المبكرة، و ذلك بتقرير نص خاص يعاقب على مجرد الأعمال التحضيرية أو ما يعرف في التشريع الجزائري بجمعيات الأشرار1.

و فضلا عن تقريره العقاب على المرحلة التي تتبع الأعمال التحضيرية إذا كانت الجريمة تشكل جنحة، نجده وسع من نطاق العقوبة نظرا لخطورة الجرائم الماسة بأنظمة المعالجة الآلية، لتشمل الأشخاص الذين يشاركون في التحضير لهذه الجرائم في إطار الاتفاق الجنائي أو أعمال البدء و الشروع.

ومن ثم فإننا نلمس مدى رغبة المشرع الجزائري في مكافحة هذه الجرائم و الوقاية منها، فالعقاب على الاتفاق الجنائي أو الشروع يغلق باب كل الأفعال سواء الماسة بأنظمة المعالجة الآلية للمعطيات أو بالأمن المعلوماتي لذا ارتأينا التطرق إلى كل من المعاقبة على الاتفاق و الشروع على الشكل الأتي:

الفرع الأول: المعاقبة على الاتفاق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise ».

[1]- أ. **رشيدة بوكر**، المرجع السابق، ص 339.

حدد قانون العقوبات[1] أنه يعد اتفاقا جنائيا كل اتفاق بين شخصين أو أكثر على ارتكاب جناية أو جنحة، سواء كانت هذه الجرائم معينة أو غير معينة أو على الأفعال المجهزة أو المسهلة لارتكابها متى ما كان هذا الاتفاق منظما و مستمرا ولو لمدة قصيرة.

كما لجأت العديد من المشرعين[2] إلى تجريمه و من بينهم المشرع الجزائري بإعتباره جريمة مستقلة بذاتها من جهة و من جهة أخرى كونها تعاقب على مجرد الأعمال التحضيرية، و قبل الفصل في موقف المشرع الجزائري و التشريعات المقارنة من تقرير عقوبة الاتفاق الجنائي، نتطرق أولا إلى الجدل الفقهي الذي ثار حول مدى ملائمة تجريم المشرع للإتفاق الجنائي من عدمه حيث ظهر هناك اتجاهان كالأتي:

فذهب اتجاه الاول[3] إلى القول أن الاتفاق الجنائي عزم إجرامي، و تجريمه لا يعتبر استثناء يرد على قاعدة "عدم العقاب على مجرد العزم الإجرامي" ، و يستند هذا الرأي إلى أن المشرع لا يعاقب على الاتفاق الجنائي كخطوة للجريمة المتفق عليها و إنما يعاقب عليه في حد ذاته كجريمة خاصة تامة، و حجة تبرير المعاقبة عليه أنه في الاتفاق الجنائي يظهر العزم الإجرامي الجماعي بمظهر خارجي مادي لأن كل عضو فيه يعلن عزمه إلى سائر الأعضاء فتتحد إرادتهم على ارتكاب الجريمة، و بذلك يكون الاتفاق معلوما و يمكن إثباته، و من جهة ثانية الاتفاق الجنائي ظاهرة خطير تهدد الأمن العام تهديدا فعليا، كما أن هدف المشرع من العقاب على الاتفاق هو الوقاية حيث أن إحباط الاتفاق الجنائي نتيجته هي الحيلولة بين الجناة و بين تحقيق خططهم الإجرامية.

و يرى أصحاب هذا الإتجاه أنه لا مجال للاعتراض على تجريم الإتفاق الجنائي بحجة أن في ذلك حث للجناة على الإقدام على ارتكاب الجرائم المتفق عليها مادام أن العقاب يقع لأول مبادرة

---

[1] - المادة 176 من قانون العقوبات الجزائري المعدل و المتمم.

[2] - جرم المشرع الفرنسي الاتفاق الجنائي في قانون العقوبات بموجب المادة 450-1 من الباب الخامس من الكتاب الرابع تحت عنوان " المشاركة في جمعيات الأشرار" de la participation à une association de malfaiteurs.

[3] - **XAVIER** Linant de bellefonds et **ALAIN** hollande ,Pratique du droit de l'informatique, 4e éd, DELMAS, 1998, p 239. مشار إليه لدى: **محمد خليفة**، مرجع سابق، ص 113.

بدرت منهم و هي اتفاقهم، و أن باب العدول الفردي مفتوح و ذلك بالتبليغ و الإخبار و ما يتبعه ذلك من إعفاء من العقاب[1].

في حين يرى اتجاه آخر[2] أن تجريم مجرد الاتفاق فقط ستكون له انعكاسات سلبية، ذلك لما يخلقه من دفع للمجرمين بإتمام ما تم الاتفاق عليه نظرا لأن اتفاقهم قد تم تجريمه حيث أن العدول عن هذا الاتفاق وفقا للرأي السابق لا يمنع من تقرير العقوبة، لأن الاتفاق حسبهم جريمة مستقلة بذاتها لذلك ذهب هذا الاتجاه للقول بأن حجج الرأي السابق غير قويمة ويكفي لدحضها جميعا المقارنة بين خطورة الاتفاق الجنائي على نحو ما صوره أصحاب الاتجاه السابق، و بين خطورة الأعمال التحضيرية التي تصدر عن شخص يسعى إلى ارتكاب الجريمة بمفرده، فالاتفاق الجنائي في مرحلة مبكرة بالنسبة للتحضير للجريمة إذ أنها ترد إلى المرحلة النفسية أي إلى مرحلة اتخاذ القرار و عقد العزم على ارتكاب الجريمة، بينما يعقب التحضير للجريمة هذه المرحلة النفسية لهذا- يضيف أصحاب هذا الاتجاه- أنه لو صحت خطورة الاتفاق الجنائي تبريرا لمعاقبة المتفقين في هذه المرحلة المبكرة من المراحل التي تمر بها الجريمة، لوجب على المشرع أن يجرم مرحلة التحضير للجريمة من باب أولى.

ذلك ما تنبه له كل من المشرع الجزائري و الفرنسي من خلال اشتراطهما أن يكون التحضير مجسدا بأفعال مادية، و ليس مجرد العزم و التصميم على الإعداد لجرائم الاعتداء على نظم المعالجة الآلية، أي تجنب المشرع العقاب على المرحلة النفسية، و هو ما يستفاذ بوضوح من نص المواد 394 مكرر 5 عقوبات جزائري و المادة 323-4 من قانون العقوبات الفرنسي المعدل و المتمم.

و للإلمام أكثر بجريمة الاتفاق الجنائي في مجال جرائم الاعتداء على نظم المعالجة الآلية للمعطيات، نتطرق إلى الأركان المكونة لها و الجزاء المقرر لهذه الجريمة من خلال النقاط الآتية:

البند الأول: الركن المادي للاتفاق الجنائي

من خلال المادة 394 مكرر 5 عقوبات جزائري يتضح أن الركن المادي لهذه الجريمة يشتمل على ثلاث عناصر تتمثل في فعل الاتفاق و تعدد المتفقين و موضوع الاتفاق.

---

[1]- يستفيد من العذر المعفى وفقا للشروط المقررة في **المادة 52** من يقوم من الجناة بالكشف للسلطات عن الاتفاق الذي تم أو عن وجود الجمعية و ذلك قبل أي شروع في الجناية موضوع الجمعية أو الاتفاق و قبل البدء **من قانون العقوبات الجزائري المعدل و المتمم** .

[2]- مشار اليه لدى: **محمد خليفة**، مرجع سابق، ص 113

أولا: فعل الاتفاق

الأصل العام في الاتفاق هو اجتماع إرادتين أو أكثر على موضوع معين، و لقد جاء في المادة 176 عقوبات جزائري انه : " كل جمعية أو اتفاق مهما كانت مدته وعدد أعضائه تشكل وتؤلف بغرض الإعداد لجناية أو أكثر، أو لجنحة أو أكثر، معاقب عليها بخمس(05) سنوات حبس على الأقل، ضد الأشخاص أو الأملاك تكون جمعية أشرار، و تقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل " غير أن المشرع الجزائري لم يخضع فعل الاتفاق في جرائم المساس بأنظمة المعالجة الآلية للمعطيات للحكم العام لهذه المادة و إنما أخضع الفعل لنص المادة 394مكرر 5 عقوبات.

و عليه قضت المادة 176 عقوبات جزائري أن فعل الاتفاق هو انعقاد أو تلاقي إرادتين أو أكثر واجتماعهما على ارتكاب الجريمة، أما المادة 394 مكرر 5 عقوبات لم تكتف بمجرد الاتفاق بل اشترطت أن يكون التحضير أو الاتفاق مجسدا بفعل أو عدة أفعال مادية، حيث تنصت على أنه:" كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها "

و هذه المادة تقابلها المادة[1] 323-4 عقوبات فرنسي، حيث يشترط المشرع الفرنسي كذلك ضرورة توافر أعمال مادية تحضيرية تعقب الاتفاق، إلا أن المشرع الفرنسي لم يقصر تجسيد ذلك الاتفاق في أفعال مادية لارتكاب جرائم الماسة بأنظمة المعالجة الآلية و إنما وسع من نطاق الاتفاق و اشترط نفس الأمر حتى في الحكم العام للاتفاق الجنائي على خلاف المشرع الجزائري و ذلك بموجب المادة 450-1 من نفس القانون[2].

[1] -**Art 323-4 du C.P.F** ; « La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée » Modifié par *Loi n°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004*

[2] -**Art 450-1 du C.P.F** ;« Constitue une association de malfaiteurs tout groupement formé ou entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'un ou plusieurs crimes ou d'un ou plusieurs délits punis d'au moins cinq ans

و قد أثار مفهوم المادية جدلا فقهيا و في ما مدى اعتبار الأعمال المادية قد تحقق فقط في صورة بدء تنفيذ الأعمال التحضيرية؟

إن جانب من الفقه الفرنسي[1] قال أنه من الواجب إعطاء مفهوم أوسع للمادية حيث أن مجرد تبادل المعلومات في صورة مناسبة بحيث يؤدي ذلك إلى تحقيق الجرائم المنصوص عليها، يعد كافيا لقيام هذه الجريمة، ومن أمثلة الأعمال التحضيرية في مجال المعلوماتية تبادل المعلومات الهامة لارتكاب الجريمة كالكشف عن رمز الاستخدام أو عبارات الدخول إلى نظام معلوماتي.

ثانيا: تعدد المتفقين أو الجناة

جريمة الاتفاق تتطلب تعددا ضروريا للجناة و أن تكون إرادتهم جادة و كلا منها محلا لاعتداد القانون بها[2]، إضافة إلى ذلك و لقيام جريمة الاتفاق يتعين أن تتجه إرادة المتفقين إلى نفس جرائم الاعتداء على نظم المعالجة الآلية و أن تتلاقى عنده متحدتً و إلا لا قيام للجريمة.

و الحد الأدنى لهذا التعداد هو شخصان بينما لا يرد قيد على الحد الأقصى حسب نص المادة 176عقوبات جزائري، و المادة 394مكرر 5 أو من المادة 323-4 عقوبات فرنسي .

و المهم في ذلك أن يتم الاتفاق بين شخصين على الأقل، فإذا ارتكب العمل التحضيري المادي شخص واحد بمفرده و بمعزل عن غيره فلا يعاقب في هذه الحالة، فالعقاب لا يتقرر إلا في حالة اجتماع شخصين أو أكثر.

ثالثا: موضوع الاتفاق

---

d'emprisonnement .Lorsque les infractions préparées sont des crimes ou des délits punis de dix ans d'emprisonnement, la participation à une association de malfaiteurs est punie de dix ans d'emprisonnement et de 150 000 euros d'amende.

Lorsque les infractions préparées sont des délits punis d'au moins cinq ans d'emprisonnement, la participation à une association de malfaiteurs est punie de cinq ans d'emprisonnement et de 75 000 euros d'amende » Modifié par ***Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002***

[1]- مشار اليه لدى: د.**عمر أبو الفتوح عبد العظيم الحمامي**، مرجع سابق، ص 1021.

[2]- **رشيدة بوكر**، مرجع سابق، ص 345.

يكتسي الاتفاق صفته الإجرامية من موضوعه فإذا لم تكن لموضوعه صفة إجرامية أي كان فعلا مشروعا و لم تكن له صلة بجريمة ما، فلا يعد الاتفاق جريمة[1]، و الملاحظ أن نص المادة 176 من قانون العقوبات الجزائري، التي نصت على الاتفاق الجنائي العام في الجنايات أو الجنح ضد الأشخاص أو الأملاك تجرم الاتفاق المنصب على ارتكاب جريمة أو الإعداد لها، و لا شك أن جرائم الإعتداء على نظم المعالجة الآلية تعد جنح ترتكب ضد الأملاك، و هو ما يجعل البعض يتساءل عن سبب نص المشرع لحكم خاص بها في المادة 394 مكرر5 مادام النص العام قد يشملها؟

إن المتمعن بنص المادة 176 السالفة الذكر قد يلاحظ أن موضوع الاتفاق يستهدف الإعداد للجنايات و الجنح المعاقب عليها بخمس (05) سنوات حبس على الأقل، بينما اقتصر نص المادة 394 مكرر 5 تجريم الاتفاق في جرائم المساس بأنظمة المعالجة الآلية للمعطيات حيث لا يتجاوز الحبس فيها ثلاثة (03) سنوات كحد أقصى، و هذا ما تفطن له المشرع و استدركه بنص خاص لتجريم الاتفاق الجنائي.

و الجنح التي يشكل تحضيرها هدف الاتفاق المنصوص عليه بالمادة 394 مكرر 5 قانون العقوبات هي فقط الجنح الماسة بأنظمة المعالجة الآلية للمعطيات، و عليه لا يعاقب استنادا إلى هذا النص الاتفاق بهدف ارتكاب جنح أخرى غير المنصوص عليها في المواد من 394 مكرر إلى 394 مكرر 2 كالسرقة أو التزوير المعلوماتي.

الأمر نفسه بالنسبة للمشرع الفرنسي بخصوص موضوع الاتفاق يجب أن يتمثل في أعمال التحضير والإعداد للجرائم المنصوص عليها من المواد 323-1 إلى 323-3-1 عقوبات فرنسي.

و عليه متى كان موضوع الاتفاق يتمثل في التحضير و الإعداد للجرائم محل الدراسة والمحدد بالنصوص القانونية السالفة الذكر، فان الاتفاق يكتسب صفته الإجرامية حتى ولو كانت الأعمال في ذاتها مشروعة، فالاتفاق على تعليم كيفية تصميم المعطيات وتجميعها ونشرها هو مشروع في الأصل لكنه يصبح غير مشروع إذا كان الاتفاق على تعليم ذلك بغية استعماله في الإجرام[2]

---

[1]- **محمد خليفة**، مرجع سابق، ص 115.

[2] - **طعباش أمين**، الحماية الجنائية للمعاملات الإلكترونية، رسالة ماجستير في القانون العام تخصص علم اللإجرام و علم العقاب، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر، باتنة، 2013/2012، ص149/ كذا: **محمد خليفة**، مرجع سابق، ص 115.

خاصة الأفعال التي نصت عليها المواد من 394 مكرر 394 مكرر عقوبات جزائري، و المواد 323-1 إلى 323-3-1 عقوبات فرنسي.

كما انه لا يشترط أن يكون موضوع الاتفاق الجنائي هو الإعداد لعدة جرائم من الجرائم السابقة، بل يكفي أن يشمل موضوعه على واحدة منها و هذا ما يستفاد من نص المادة 394 مكرر بقولها " ... لجريمة أو أكثر......"

البند الثاني: الركن المعنوي للاتفاق الجنائي

الاتفاق جريمة عمدية يشترط لقيامها توافر قصد جنائي و هذا الأخير يقوم على عنصرين هما العلم و الإرادة.

أولا: العلم

يلزم لتوافر القصد الجنائي ان يعلم كل عضو في الجماعة بماهية الفعل أو الأفعال موضوع الاتفاق، و بما لها من خصائص يعتمد عليها المشرع في إضفاء الصفة الإجرامية عليها[1]، أي توافر العلم لدى كل منهم بأنه عضو في جماعة إجرامية و أن الغرض من الاتفاق هو ارتكاب جنح الاعتداء على نظام المعالجة الآلية أو التحضير لها، أما من جهل الغرض من ذلك لا يعد القصد الجرمي متوفرا من جانبه؛

كما إذا انضم عضو إلى الاتفاق معتقدا انه الاتجار في برامج معلوماتية أو معلومات عادية، فإذا به للاتجار في برامج غير مشروعة أو برامج خبيثة مثل البرامج الفيروسية، أو البرامج الإختراق[2] فبانتفاء علمه بموضوع الاتفاق لا يتوفر القصد الجنائي لديه، ولكنه يتوافر فيه القصد إذا علم هذا العضو بعد دخوله الاتفاق بموضوعه غير المشروعية ومع ذلك بقي في الاتفاق[3]، و عليه يلزم وعي الشخص بمشاركته باتفاق بغرض الإعداد لارتكاب إحدى الجرائم الماسة بأنظمة المعالجة الآلية.

ثانيا: الإرادة

---

[1]- **احمد خليفة**، مرجع سابق، ص 117.

[2] - **رشيدة بوكر**، مرجع سابق ص348.

[3] - **محمد خليفة**، مرجع سابق، ص117/ **طعباش أمين**، مرجع سابق، ص151

إضافة إلى علم كل عضو من أعضاء الاتفاق بموضوع الاشتراك فيه فانه لابد أن تتجه كذلك إرادة كل عضو إلى تحقيق نشاط إجرامي معين يتمثل في العمل التحضيري لتلك الجرائم المنصوص عليها[1].

وعليه فانه يجب أن تتوفر الإرادة الجادة لشخصين على الأقل للدخول في الاتفاق، أي إرادة كل واحد و يكون طرفا في هذا الاتفاق، و أن يقوم بالدور الذي سيعهد به إليه، فإذا لم تكن الإرادة جادة[2] و كان دخول الاتفاق لمجرد الوثوق بأعضاء المجموعة أو لمجرد الاطلاع على أمرهم دون الانضمام إليهم أو كان لمجرد العبث، فانه ينتفي عنه القصد الجنائي لانتفاء الإرادة الجادة.

و لا شك أن تجريم المشرع الجزائري للاتفاق الجنائي بغرض الإعداد لجريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات قد يكون من ورائه حكمة، ذلك أن مثل هذه الجرائم تتم عادة في إطار مجموعات لتبادل و جمع المعلومات ، إضافة إلى رغبة المشرع في توسيع نطاق العقوبة فأخضع حتى الأعمال التحضيرية التي تسبق البدء في تنفيذ هذه الجرائم إلى العقاب.

البند الثالث:عقوبات الاتفاق الجنائي

حسب ما جاء في المادة 394 مكرر5- فان المشرع[3]يعاقب على الاشتراك في الاتفاق الجنائي بنفس عقوبة الجريمة التي تم الإعداد والتحضير لها و ذلك ما يظهر بوضوح من العبارة الواردة في المادة السابقة "....يعاقب بالعقوبات المقررة لجريمة ذاتها..."

وما يمكن ملاحظته من ذلك أيضا أن المشروع لم يحدد العقوبة في حالة تم التحضير والإعداد لارتكاب عدة جرائم من الجرائم الماسة بأنظمة المعالجة الآلية كإعداد لارتكاب جريمة

1- **سوير سفيان**، جرائم المعلوماتية ، مذكرة ماجستير في العلوم الجنائية و علم الإجرام، كلية الحقوق و العلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2010/2011، ص102 .

2- **د.علي عبد القادر القهوجي**، الحماية الجنائية لبرامج الحاسب الالي، الدار الجامعية للنشر و التوزيع، الإسكندرية، 1999، ص 129 / **احمد خليفة**، مرجع سابق، ص117.

3- بالرجوع إلى الأحكام العامة الواردة بشان العقاب على الاتفاق الجنائي العام فان المشرع حدد العقوبات على أساس خطورة الجريمة من خلال **المادة 177 قانون العقوبات الجزائري المعدل و المتمم** و التي جاء فيها "يعاقب على الاشتراك في جمعية الأشرار بالسجن المؤقت من خمس (5) سنوات إلى عشر(10) سنوات و بغرامة من 500.000 دج إلى 1.000.000 د.ج، إذا تم الإعداد لارتكاب جنايات.

و تكون العقوبة الحبس من سنتين(2) إلى خمس (5) سنوات و الغرامة من 100.000 دج إلى 500.000 دج إذا تم الإعداد لارتكاب جنح ".

الدخول أو البقاء غير المصرح و كذلك التلاعب بالمعطيات وأنظمة المعالجة الآلية أو نشر المعلومات المتحصل عليها من اختراق النظام.

و في هذه الحالة يمكن الرجوع إلى الأحكام العامة في حالة تعدد الجرائم من فاعل واحد وبذلك تطبق عليه العقوبة الأشد.

و هذا ما أقره المشرع الفرنسي صراحة و أورده في أخر عبارة من المادة 323-4 بقوله "......او بعقوبة الجريمة الأشد": "Ou pour l'infraction la plus sévèrement réprimée"

و تطبق العقوبة حتى في حالة عدم إتمام الجريمة التي تم الإعداد لها، ذلك أن جريمة الاتفاق جريمة مستقلة بذاتها عن الجرائم الأخرى و تقوم بمجرد الاتفاق[1].

الفرع الثاني: المعاقبة على الشروع في الجرائم المعلوماتية

نصت على الشروع المادة 11 من اتفاقية بودابست للإجرام الالكتروني[(2)]، و تبناه كذلك المشرع الجزائري في نص المادة 394 مكرر 7 من قانون العقوبات.

ويراد بالشروع "tentative" في الجريمة ذلك السلوك الذي يهدف به صاحبه إلى ارتكاب جريمة معينة، كانت لتقع بالفعل لو لا تدخل عامل خارج عن إرادة الفاعل حال دون وقوعها في أخر لحظة [(3)]

إن الأصل في المعاقبة على الشروع يكون في مجال الجنايات فقط آما الجنح فلا يكون إلا بنص صريح و في الجنح الخطيرة منها، و لقد تطرق المشرع الجزائري للشروع في قانون العقوبات تحت مسمى المحاولة، من خلال المادة 30 منه و التي تنص بأنه: " كل محاولة لجناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية نفسها إذا لم توقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها.."

---

[1] - **عمر ابو الفتوح عبد العظيم الحمامي**، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دراسة مقارنة ، دار النهضة العربية، القاهرة، 2010، ص 10،22.

[2]- ورد التنصيص على الشروع كذلك في **الإتفاقية العربية لمكافحة جرائم تقنية المعلومات** الموقعة بالقاهرة و المصادق عليها مؤخرا من طرف الجزائر بموجب مرسوم رئاسيّ رقم **14-252 مؤرّخ في 8 سبتمبر يتضمّن التّصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحرّرة بالقاهرة بتاريخ 21 ديسمبر سنة 2010**، ج.ر عدد **57** بتاريخ **28** سبتمبر **2014**.، في المادة **2/19** مع حق الدول الأطراف في عدم تطبيق هذه الفقرة جزئيا أو كليا.

[3] - **د.طارق ابراهيم الدسوقي عطية**، الأمن المعلوماتي- النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2009، ص 184.

و كذلك ما جاء في نص المادة 31 من نفس القانون "المحاولة في الجنح لا يعاقب عليها إلا بناء على نص صريح في القانون والمحاولة في المخالفة لا يعاقب عليها إطلاقا".

و بالتالي إذا كان المشرع قد جرم و عاقب على مرحلة الاتفاق الجنائي في الأعمال التحضيرية بصفتها مرحلة تسبق مرحلة الشروع، فمن المنطقي تجريم مرحلة الشروع بوصفها مرحلة البدء في التنفيذ.

ونفس الآمر يقال بشأن المشرع الفرنسي حيث عاقب على الشروع بموجب المادة 323-7 عقوبات فرنسي[1].

تعتبر الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من الجنح الخطيرة التي أخضعها التشريع الجزائري و التشريعات المقارنة[2] لنظام الاتفاق الجنائي المجسد بأعمال مادية ثم لنظام الشروع أيضا، و لهذا الأخير كذلك أركان محددة و عقوبة مقررة نستشف ذلك من خلال العناصر الآتية:

البند الأول: الركن المادي

يقوم الركن المادي في الشروع في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات على عنصرين اثنين هما:

أولا: البدء في التنفيذ

البدء في التنفيذ مرحلة تأتي بعد التفكير في ارتكاب جريمة من الجرائم الماسة بقواعد الأمن المعلوماتي أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، و مرحلة التحضير لها إذ يبدأ الجاني في تنفيذ الجريمة بالقيام بفعل مادي في سبيل تنفيذها، ويكون بذلك قد دخل في نطاق الشروع، غير أن الإشكال الذي ثار كان بشان تحديد مرحلة بدئ التنفيذ عن المراحل التي تسبقها وخاصة ان المرحلة التحضيرية لا عقاب عليها إلا إذا اتخذت مظهرا ماديا وفق ما سبق بيانه حيث اختلف الفقه حول تحديد معيار البدء في تنفيذ و انقسم إلى مذهبان:

---

[1] **Art 323-7 Du C.P.F** ; « La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines » Modifié ***par Loi n°2004-575 du 21 juin 2004*** art. 46 JORF 22 juin 2004.

[2] - إن المشرع الأردني رغم وضعه لقانون مؤقت لجرائم أنظمة المعلومات إلا أنه على خلاف المشرع الجزائري و الفرنسي لم يعاقب على الشروع في هذه الجرائم.

المذهب المادي أو الموضوعي طبقا لهذا المذهب فان البدء في التنفيذ هو أن يكون الفاعل قد حقق عملا للبدء في الركن المادي للجريمة، فاذا لم يدخل الجاني بفعله الى الركن المادي، فلا يعتبر سلوكه بدء في التنفيذ ولا شروعا في الجريمة ولا يناله العقاب[1]، فلا يعد الشخص مثلا شارعا في السرقة إذا لم يكن قد وضع يده على المال الذي يريد أن يختلسه[2] .

و قد أخد على هذا المذهب أنه يترك بدون عقاب جناة هم أهل العقاب رغم خطورة أفعالهم.

المذهب الشخصي: يذهب أنصاره و على رأسهم الفقيه " Garraud " إلى القول بأن الشروع هو سلوك يؤدى حالا و مباشرة إلى الركن المادي للجريمة، كما وصفها نموذجها في القانون، و لو لم يكن السلوك قد حقق بالفعل بداية هذا الركن.

و لا يلزم على ذلك اعتبار شخص ما شارعا في السرقة أن يكون قد حاز بالفعل المال المنقول المقصود بالسرقة، و إنما يكفي أن يكون قد بلغ في السلوك حدا يؤدي حالا و مباشرة إلى هذه الحيازة [3] و بالتالي عليه الإتيان بفعل يؤدي مباشرتا إلى النتيجة المقصودة.

و قد انتقدت صياغة هذا المذهب من قبل الأستاذ " Roux " من ناحية أن الفعل قد لا يؤدي في الحال إلى الركن المادي للجريمة و إنما قد يستغرق في سبيل بلوغ هذا الركن مدة من الوقت أو أياما، و من ثم الاكتفاء في تعريف الشروع بأنه:" العمل المؤدى مباشرة إلى ارتكاب الجريمة"[4]

قد استقر القضاء الفرنسي على الأخذ بالمذهب الشخصي و على ترديد صياغته في التعريف بالشروع [5] .

أما عن موقف المشرع الجزائري فقد تأثر في ذلك بالاتجاه الغالب في معظم التشريعات و في مقدمتها التشريع الفرنسي الذي اعتمد المذهب الشخصي، كما استفاد من العبارة ذاتها المكرسة من قبل القضاء الفرنسي و يظهر ذلك من خلال العبارات الواردة بالمادة 30 عقوبات جزائري "...بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها...".

من ثم فان الشروع في تنفيذ وهو العمل المؤدي مباشرة الى ارتكاب الجريمة.

1- **عمر أبو الفتوح عبد العظيم الحمامي**، مرجع سابق ص 1007.

2- د.**طارق إبراهيم الدسوقي عطية**، مرجع سابق، ص186.

3 - نفس المرجع، ص 186.

4 - **رشيدة بوكر**، مرجع سابق، ص 354/د.**طارق ابراهيم دسوقي عطية**، مرجع سابق ص187.

5 -**عمر أبو الفتوح عبد العظيم الحمامي**، مرجع سابق، ص1008.

وتطبيقا لذلك هل يمكن تصور الشروع في نطاق الجرائم الماسة بقواعد الأمن المعلوماتي بصافة عامة و جرائم المساس بأنظمة المعالجة الآلية للمعطيات كما جاء بها المشرع الجزائري؟

أن موقف المشرع الجزائري كان جليا فيما يخص الشروع في الجريمة بصفة عامة، و على خلاف ذلك بالنسبة لجرائم المساس بأنظمة المعالجة الآلية للمعطيات، حيث جرم المشرع الجزائري معظم الأعمال التحضيرية لهذه الجرائم نظرا لخطورتها و باعتبارها جرائم مستقلة قائمة بذاتها وذلك من خلال المادة 394 مكرر 2 عقوبات.

غير أنه لا يتصور دائما الشروع في جميع جرائم الاعتداء على النظم، من ذلك جريمة الدخول غير المصرح به و على اعتبار أنها من الجرائم الشكلية فإنه وفقا للأحكام العامة لا يمكن الحديث عن الشروع فيها، فلكي يكون هناك مجال للقول بخيبة الأثر لابد أن يكون هناك نتيجة، أو عدم تحققها لظروف خارجة عن إرادة الفاعل، و بالتالي فالجرائم الشكلية إما أن تقع بوقوع الفعل فتعتبر جريمة تامة و إما أن لا تقع أبدا.

و عليه إذا كان موقف المشرع الجزائري واضحا بشان تجريم الشروع في كل الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بدون استثناء إلا انه من الصعب تصوره في كل تلك الجرائم، و مع ذلك نجده قد ختم في المادة 394 مكرر بعبارة" ...أو يحاول ذلك".

وهذا ما تنبهت له اتفاقية بودابست بإشارتها إلى صعوبة تصور الشروع في بعض عناصر الجرائم التي تستهدف امن المعلومات, وتأسيسا على ذلك فان الأطراف الموقعة على الاتفاقية لا يلزمون بتجريم الشروع إلا في الجرائم المحددة في بعض المواد، كما انه ليس ملزم بتجريم الشروع المرتكب في كل جريمة منصوص عليها في هذه الاتفاقية[1]

ومن الجرائم التي استثنت الاتفاقية بودابست عدم تجريم الشروع فيها نظرا لصعوبته، نجد جريمة الدخول غير مصرح و لعل ذلك يرجع إلى صعوبة معرفة أو تحديد الأفعال التي تدخل في نطاق البدء في التنفيذ وتميزها عن الأعمال التحضيرية الغير معاقب عليها من محاولة الدخول إلى النظام المعلوماتي.

والأمر ذاته بالنسبة للاتفاقية العربية بشان مكافحة جرائم تقنية المعلومات و ما جاءت به الفقرة الثالثة من المادة 19 من ذات الاتفاقية.

ثانيا: خيبة أثر الجريمة نتيجة ظروف خارجة عن إرادة الفاعل.

1- **هلالي عبد الله احمد**، مرجع سابق ص 146-147.

حسب المادة 30 من قانون العقوبات جزائري فإنه للحديث عن الشروع فانه لا يكفي البدء في التنفيذ وإنما يتطلب الأمر وقف التنفيذ أو خيبة اثر الفعل لأسباب خارجة عن الفاعل لا دخل لإدارته فيها بقولها "... إذا لم توقف أو لم يخب أثرها إلا لظروف مستقلة عن إرادة مرتكبها..."

و إذا كان تحديد الشروع المعاقب عليه تعترضه بعض الصعوبات حيث لا يوقف الفاعل في إتمام سلوكه الى النهاية لتدخل عوامل خارجة عن إرادته حالت دون ذلك، فانه لا صعوبة في ذلك التحديد في حالة كان الفاعل قد مضى في سلوكه إلى النهاية و بدون عائق غير أن الحدث الذي كان يراد تحقيقه هو الذي تأثر بالعامل الذي حال دون وقوعه[1].

وفي الحالتين لا تحدث الجريمة على الصورة الكاملة المطابقة لنموذجها وعلى ذلك نفرق بين الجريمة التامة و الشروع في الجريمة.

نقول أن الجريمة تامة عندما تكتمل جميع أركانها وعناصرها المحددة بالنص القانوني المعاقب عليها، فيتحقق الركن المادي والمعنوي والنتيجة التي يريدها الجاني إذا كان من الجرائم المادية، أما الشروع فيختلف عن الجريمة في تحقيق النتيجة، حيث إذا لم تتوفر هذه الأخيرة رغم تحقق العناصر الأخرى اعتبر الأمر شروعا في الجريمة[2]

الأصل في القواعد العامة التقليدية انه لا شروع في الجرائم الشكلية غير أننا نجد المشرع الفرنسي و تبعه في ذلك المشرع الجزائري قد خرج عن هذه القواعد كما سبق بيانه ، وعاقب على الشروع في الجرائم الشكلية في نطاق الماس بأنظمة المعالجة الآلية للمعطيات و ذلك ما يستفاد من 323-7 قانون العقوبات فرنسي و المادة 394 مكرر 05 عقوبات جزائري[3].

البند الثاني: الركن المعنوي

---

[1]- هناك فرق بين الجريمة الناقصة أو الشروع التام والجريمة الموقوفة أو الناقصة، في الأصل لا تحقق الجريمة على الصورة الكاملة المطابقة لنموذجها الموصوف في القاعدة الجنائية إذ لا يتوفر منها سوى السلوك، و في الحالة الثانية أو في الجريمة الموقوفة لا يتوفر منها سوى جزء من السلوك اللازم لارتكابها، و من اجل ذلك يطلق على الشروع في الحالتين اسم الجريمة الناقصة: لمزيد من التفاصيل لدى **د.طارق ابراهيم الدسوقي عطية**، مرجع سابق، ص190.

[2] - **عمر أبو الفتوح عبد العظيم الحمامي**، مرجع سابق ص 1009.

[3] - بعض التشريعات العربية و منها **التشريع الأردني** على خلاف **المشرع الجزائري** لم تنص على المعاقبة على الشروع في هذا النوع من الجرائم

الشروع جريمة عمديه[1] يتخذ فيها الركن المعنوي صورة القصد بعنصريه العلم و الإرادة و لا يختلف هذا الركن الخاص بجريمة الشروع عن الركن المعنوي في الجريمة التامة و هو ما يقتضي اتجاه الإرادة إلى ارتكاب الجريمة لا إلى مجرد الشروع فيها.

و على ذلك يكون سلوك الجاني إراديا، و ان يتوافر علمه بكافة العناصر الجوهرية اللازمة قانونيا لقيام الجريمة، و ان تتوفر لديه نية تحقيق النتيجة[2].

مع الإشارة إلى انه إذا كانت جريمة الشروع من الجرائم القصد الخاص، فلا بد أن يتوافر لدى الجاني هذا القصد.

البند الثالث: المعاقبة على الشروع:

وفقا للمادة 30 من قانون العقوبات السابقة الذكر، فإن المشرع الجزائري جعل الشروع في الجناية كالجناية نفسها، و بالتالي يعاقب عليها بنفس العقوبة المحددة قانونا للجناية، أما بالنسبة للجنح فانه لا عقاب على الشروع فيها إلا بنص صريح[3]، و هذا ما استدركه فيما يخص الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بالعقاب على الشروع فيها بالعقوبات المقررة للجنحة ذاتها، ولا شك أن تقرير المشرع الجزائري العقاب على الشروع في هذا النوع من الجرائم قد يرجع إلى إدراكه لخطورتها وخصوصيتها، و إلى ما قد تؤدي إليه من خسائر في حالة إتمامها.

وهو ما اقره المشرع الفرنسي كذلك و ذلك بموجب المادة 323-7 عقوبات.

غير أن الفرق بين التشريعين أن المشرع الجزائري من خلال المادة 394 مكرر 7[4] عاقب على الشروع في كل الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بما في ذلك المادة التي تعاقب على الاتفاق الجنائي و وسع بذلك من نطاق العقاب على الشروع ليشمل حتى الاتفاق الجنائي، أما بالنسبة للمشرع الفرنسي فقد أخرجه من دائرة العقاب على الشروع من خلال المادة 323-7[5] والتي اقتصرت العقاب على الشروع في الجرائم المنصوص عليها في المواد من 323-1 إلى 323 -3-1.

---

[1]- وهذا مانصت عليه المادة 2/11 من اتفاقية بودابست

[2]- **طارق ابراهيم دسوقي عطية**، مرجع سابق، ص 193.

[3]- المادة 1/31 من **قانون العقوبات الجزائري** المعدل والمتمم.

[4]- تنص المادة 394 مكرر 7 عقوبات جزائري على أنه:: يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".

[5]- **Art 323-7 Du C.P.F** dispose que : « La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines ».

الخاتمة:

إن النصوص التشريعية الموضوعية و التي جاء بها المشرع الجزائري من التعديلات الأخيرة للقوانين العقابية أظهرت عدم كفايتها لمواجهة أخطار و مهددات أمن الأنظمة المعلوماتية، و أن بعض الجرائم التقليدية التي قد تحدث بإستعمال وسائل الاتصال الحديثة او التي لا تنفذ الا باستخدام الحاسب الآلي، أو بواسطة أنظمة معلوماتية مثل السرقة المعلوماتية و التزوير المعلوماتي لا تنطبق عليها تلك التعديلات و لا يمكن معاقبة فاعليها بالنصوص التي نظمت الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات مما يستدعي استدراك المشرع لبعض أشكال الإجرام التقليدي التي تقع بواسطة أنظمة معلوماتية أو جعلها مرنة بما يتناسب مع تلك الجرائم.

كما انا ازدياد حجم الجرائم المعلوماتية يوحي بعدم جدوى او عدم كفاية العقوبة لردع مرتكبيها مما يستدعي ضرورة تشديد العقاب أو البحث عن استراتيجيات كفيلة للحد من الجريمة المعلوماتية



المحور السابع

تقنيات الحد من مخاطر لجريمة المعلوماتية

حوكمة تكنولوجيا المعلومات (ITG) كآلية للحد من الجريمة المعلوماتية:

Information technology governance (I T G) as a mechanism to reduce information crime

د.مجدوب خيرة أستاذة محاضرة أ

جامعة ابن خلدون تيارت - الجزائر

مقدمة:

في ظل التطور الهائل الذي شهده مجال تكنولوجيا الإعلام والاتصال والذي رافقه التطور الكبير في تكنولوجيا الحواسيب والأجهزة الذكية، أدى ذلك إلى ظهور أدوات واختراعات وخدمات جديدة نتج عنها نوع جديد من المعاملات يسمى:" المعاملات الالكترونية" والذي يقصد بها كل المعاملات التي تتم عبر أجهزة الكترونية مثل الحاسوب، شبكة الانترنت، الهاتف المحمول(الهواتف الذكية)، ونتيجة التطور الكبير والسريع لهذه الأجهزة وضعف القدرة على المرافقة والمراقبة والتحكم ظهر نوع جديد من الجرائم يسمى بالجريمة الالكترونية أو المعلوماتية أو التقنية، والتي هي عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي أو الهواتف الذكية الموصولة بطريقة مباشرة أو غير مباشرة لتنفيذ الفعل الإجرامي، وأصبحت هذه الجرائم في وقتنا الراهن تهدد أمن وسلامة الأفراد والمؤسسات أو حتى الحكومات ، وهو ما يقتضي الإسراع في اتخاذ الإجراءات اللازمة والتي من شأنها التقليل من حدة هذا النوع من الجرائم.

ولقد واجهت منظمات الأعمال في مختلف القطاعات والأنشطة تحديات كبيرة فرضت عليها ضرورة استخدام التقنيات الحديثة والتكنولوجيا المتقدمة، إذ أصبح ذلك معيارا هاما في تطور هذه المنظمات ودافعا للتعامل معها و التنافسية في مجالات أعمالها، وقد تطلب ذلك قيام المنظمات بإنفاق أموال ضخة على الاستثمار في تكنولوجيا المعلومات وأنظمتها.

من جهة أخرى، واجهت الاستثمارات الضخمة والتقنيات المعاصرة العديد من المخاطر والتهديدات والتحديات التي صاحبتها، إذ أفرزت البيئة الجديدة عددا من المتغيرات التي لم تكن موجودة من قبل في ظل استخدام الأساليب التقليدية في منظمات الأعمال خاصة تلك التي تعتمد على النظم اليدوية وبرزت أشكال جديدة من المخاطر والجرائم المصاحبة لاستخدام التكنولوجيا والتقنيات الالكترونية.

وهنا برزت إلى الأفق "**حوكمة تكنولوجيا المعلومات**" كحل وآلية محورية للحد من آثار ومسببات الجريمة الالكترونية المنظمة وهذا نظرا للمنافع والمزايا التي تحققها على المستوى الاقتصادي الكلي وكذلك على مستوى الوحدات الاقتصادية نتيجة تطبيق قواعد ومعايير الحوكمة الرشيدة.

إشكالية الدراسة: لقد أتاح ظهور الانترنت العديد من التسهيلات لحياة أفضل وأيسر، إلا أنها حملت معها في نفس الوقت مخاطر وجرائم مست العديد من الجوانب الحياتية، وتسببت في تقلبات خطرة من الناحية الاقتصادية، بحيث يحاول المخترقون والعابثون الاستفادة قدر الإمكان من توسع استخدام الانترنت وذلك بنشر فيروساتهم المدمرة لتعطيل أجهزة الكمبيوتر الخاصة بالأفراد ومختلف المؤسسات الحكومية والخاصة وتجميد الشبكة بكاملها، ومن بين الجرائم الالكترونية الممكنة الوقوع نجد اختراق الأنظمة ومسح البيانات والقيام بالسرقات الإلكترونية وانتحال الشخصية والابتزاز ونشر الإشاعات عبر الانترنت مما يهدد سلامة وبقاء المؤسسة ويضعف تنافسيتها.

إن ضمان حماية نظم التكنولوجيا وحماية مخرجاتها، استدعت ضرورة البحث عن الإجراءات الكفيلة بتحقق الإدارة الفعالة لنظم تكنولوجيا المعلومات مما دعا الباحثين للعمل على إيجاد الضوابط التي تضمن تعظيم منافع التكنولوجيا وتحمي مخرجاتها من المعلومات من العبث ، مما فتح مجال البحث في حوكمة تكنولوجيا المعلومات.

وعليه تتمثل إشكالية هذه الورقة البحثية في التساؤل الرئيسي التالي:

ما هي آليات حوكمة تكنولوجيا المعلومات المستخدمة للحد من الجريمة المعلوماتية؟

أهمية الدراسة: تعتبر هذه الورقة البحثية بمثابة مرجعية تسمح بالتعرف على الأدوات والآليات المتبعة لتحقيق الحد الأدنى لجودة وأمن المعلومات الالكترونية ومحاربة الجريمة المعلوماتية ضمن إطار حوكمة تكنولوجيا المعلومات بما يضمن زيادة جودة المعلومات وتعزيز الإجراءات الأمنية للحفاظ عليها وتدعيم الجوانب الرقابية وتحسين إدارة المخاطر المرتبطة بها وهذا ما سينعكس على زيادة ثقة المستثمرين الحاليين والمرتقبين في هذه المعلومات.

أهداف الدراسة: تهدف هذه الورقة البحثية إلى تسليط الضوء على مفهوم حوكمة التكنولوجيا المعلومات كآلية حديثة للحد من الجريمة المعلوماتية وحماية والحفاظ على أمن المعلومات ونظم المعلومات من الاستخدام غير المرخص به والإفشاء والتعديلات أو التدمير وهذا من خلال:

- المحافظة على السرية بتوفير مستوى مناسب من سرية المعلومات.

- السلامة والدقة للتأمين ضد حدوث تغيرات غير سليمة في المعلومات أو تدميرها وأن تكون المعلومات يوثق فيها وليس هناك مجال للاختلاف أو التنصل من المسؤولية عنها.
- الإتاحية بمعنى قابلية المعلومات للتداول والنفاذ إليها طوال الوقت.

منهج الدراسة: اعتمدت الدراسة على المنهج التحليلي وهذا من خلال التطرق لمفهوم الجريمة المعلوماتية على مستوى الوحدات الاقتصادية وكذا تحليل آليات حوكمة تكنولوجيا المعلومات كأحد السبل المستخدمة للوقاية منها وكضرورة في العصر الرقمي والمتمثل في الثورة الالكترونية وذلك لضمان أفضل أداء لهيكلة تقنية المعلومات كي تساند المؤسسة في تحقيق أهدافها الإستراتيجية خصوصا بعد الاعتماد شبه التام على تكنولوجيا المعلومات والاتصال في أداء الأعمال وارتباط الميزة التنافسية للمؤسسات بهذه التقنيات، وأيضا لضمان مواجهة المخاطر التي قد تتعرض لها هيكلة تكنولوجيا معلومات المؤسسة من قرصنة وتجسس وتخريب للبيانات والتي قد تؤدي إلى خسائر كبيرة زيادة على تشويه صورة المؤسسة في السوق.

تقسيمات الدراسات:ومن أجل الإلمام بجوانب الموضوع ارتأينا تقسيم ورقتنا البحثية إلى المحاور التالية:

المحور الأول:التأصيل النظري لحوكمة تكنولوجيا المعلومات والجريمة المعلوماتية.

المحور الثاني: الحاجة لحوكمة تكنولوجيا المعلومات في المؤسسة.

المحور الثالث: أساليب حوكمة تكنولوجيا المعلومات للحد من الجريمة المعلوماتية.

المحور الأول: التأصيل النظري لحوكمة تكنولوجيا المعلومات والجريمة المعلوماتية.

تختلف الشركات عن بعضها في تطبيقها لحوكمة تكنولوجيا المعلومات إذ أنها تحرص في تنافسها الشديد فيما بينها على الحصول على أفضل أداء من خلال بناء حوكمة تقود إلى الأداء الذي يمكن قياسه مثل العائد على الأصول وتصميم جيد لها يمكن الشركات من الحصول على نتائج جيدة من الاستثمار في تكنولوجيا المعلومات وبتكاليف اقل وفعالية أكبر.

أولا: مفهوم حوكمة تكنولوجيا المعلومات: تعد حوكمة تكنولوجيا المعلومات جزءا من حوكمة الشركات ذلك المفهوم الذي يحضا باهتمام بالغ على كافة المستويات - الحكومية والتشريعية وجهات الإشراف والرقابة ومؤسسات الأعمال - على حد سواء، نظرا لما كشفت عنه الدراسات والبحوث من المنافع والمزايا التي تتحقق على المستوى الاقتصادي الكلي، وكذلك على مستوى الوحدات الاقتصادية نتيجة لتطبيق قواعد ومعايير ومبادئ الحوكمة الجيدة وقد أدت المحاولات

المتعمقة بإرساء دعائم حوكمة الشركات إلى الحاجة الملحة لأحد معايير ومحاور الحوكمة، وهو ما أطلق عليه حوكمة تكنولوجيا المعلومات والذي يعد التطبيق الجيد لمبادئها وقواعدها ومنهجيتها.

وعرفت حوكمة تقنية المعلومات من قبل معهد حوكمة تقنية المعلومات على أنها " الهياكل التنظيمية والإجراءات التنفيذية والقيادية لتقنية المعلومات، المساعدة في توسيع إستراتيجية المنظمة وتحقيق أهدافها.[1]

وعرفت كذلك بأنها" القدرة التنظيمية التي يمارسها مجلس الإدارة و الإدارة التنفيذية لتقنية المعلومات في صياغة و تنفيذ إستراتيجية تقنية المعلومات والرقابة عليها بما يضمن توافق تقنية المعلومات مع أعمال المنظمة".[2]

كما تعرف على أنها: " الطاقة المنظمة للرقابة على صياغة وتنفيذ إستراتيجية تقنية المعلومات والاسترشاد بها للوصول إلى تحقيق المزايا التنافسية للمنظمة".[3]

أما المعهد الاسترالي للحوكمة فقد عرفها على أنها"النظام الذي يتم من خلاله توجيه ورقابة الاستخدامات الحالية والمستقبلية لتقنية المعلومات وتقييم وتوجيه الخطط لاستخدام تقنية المعلومات في تدعيم المنظمة ومتابعة هذا الاستخدام لانجاز الخطط و الأهداف المقررة.[4]

ثانيا:أهمية حوكمة تكنولوجيا المعلومات: تكمن أهمية تكنولوجيا المعلومات في النقاط التالية:

- إن حوكمة تقنية المعلومات تمكن الإدارة الفعالة لرغبات واحتياجات الزبائن في إطار الإستراتيجية العامة للمنظمة.

[1] Etzler, Joel:"**IT Governance According to COBIT: How Does the IT Performance Within One of the Largest Investment Banks in the World Compare to Cobit**", ***Master Thesis***, Stockholm, Sweden,2007, p 19

[2] Gelling, Cornelia. (2007). **Outsourcing Relationships: The Contract as IT Governance Tool**. Goethe University, Frankfurt, Germany. 2007,p 01

[3] Simons Son, Marten and Others: **IT Governance Decision Support Using the IT Organization Modeling and Assessment Tool**. Royal Institute of Technology, Stockholm, Sweden, 2008,p18.

[4] ثائر أحمد سعدون، محمد ضياء يونس، محمد عاصم محمد: "**متطلبات تقانة المعلومات في تعزيز الأداء الاستراتيجي للمنظمات الخدمية بالتركيز على بطاقة الأداء المتوازن: دراسة حالة في مديرية اتصالات و بريد نينوى**"، كلية الإدارة و الاقتصاد، جامعة الموصل، العراق، 2012، ص ص 45-46.

- تقوم حوكمة تقنية المعلومات بتوجيه الإدارة العليا ومشاركتها في تحقيق مصالح المتعاملين مع المنظمة.
- تزداد أهمية حوكمة تقنية المعلومات عند الرغبة في تحقيق عائد اقتصادي على جميع الأنشطة التي تقوم بها المنظمة وتحمل تكاليف مقابلها.
- تستخدم في تحسين وتطوير التقنيات المستخدمة باستمرار لتفي بالمتطلبات المتغيرة بالبيئة المحيطة.
- تقدم حوكمة تقنية المعلومات التطور السريع والمعقد في تقنية المعلومات المستخدمة في جميع المجالات.[1]
- وجود إطار وقوانين تحكم تصميم الخدمات الالكترونية وإطلاقها.
- التزام الإدارات بالمخطط التوجيهي العام الصادر عن السلطة المنوط بإدارة الحكومة الالكترونية.
- المعايير والمقاييس التي يجب أن تعتمدها الدوائر الحكومية في حال ما إذا قررت بناء أنظمة إلكترونية-حكومية.
- جودة الخدمة وكيفية قياس مدى استخدام الجمهور المستهدف لها.[2]

ثالثا: مفهوم الجريمة المعلوماتية: تولد عن ثورة الاتصالات وتكنولوجيا المعلومات العديد من التطبيقات التي أثرت لدرجة كبيرة على أوجه النشاط الاقتصادي والاجتماعي، ويكاد يتفق الفقه على سمات العالم الالكتروني وكذا صفات المجرم المعلوماتي، ولكن لا يوجد إجماع على تعريف الجريمة الإلكترونية من حيث كيف تُعرف أو ما هي الجرائم التي تتضمنها الجريمة الإلكترونية، وكما يقول فان دير هلست ووينف: هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية والرقمية.

ويتراوح تعريف الجريمة الإلكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية وتعريف الجرائم الإلكترونية باختصار على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال.

[1] حنفي حسين عادل: " حوكمة تقنية المعلومات كمدخل لحماية امن المعلومات والخصوصية بالمؤسسات الاقتصادية"، ص04 ، متاح على: www.shaimaatalla.com

[2] أحمد الكردي: " حوكمة الحكومة الالكترونية"،ص01، متاح على الموقع: www.kenanaonline.com

تتكون الجريمة الإلكترونية أو الافتراضية (cyber crimes) من مقطعين هما الجريمة (crime)والإلكترونية (cyber) ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات.

أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون والجرائم الإلكترونية هي المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت (غرف الدردشة – البريد الالكترونية – الموبايل).

وتعتمد تعاريف الجريمة الإلكتروني في الغالب على الغرض من استخدام هذا المصطلح وتشمل عددا محدداً من الأعمال ضد السرية والنزاهة وتوافر بيانات الكمبيوتر أو أنظمة ويمثل جوهر الجريمة الإلكترونية أبعد من هذا الوصف ومع ذلك، فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو تحقيق مكاسب مالية أو ضرر بما في ذلك أشكال الجرائم المتصلة بالهوية والأفعال المتعلقة بمحتويات الكمبيوتر جميعها تقع ضمن معنى أوسع لمصطلح "الجريمة الإلكترونية".[1]

المحور الثاني: الحاجة لحوكمة تكنولوجيا المعلومات في المؤسسة:

هناك عدة أسباب رئيسية تحتم على المؤسسة تطبيق حوكمة على تكنولوجيا وتقنيات معلوماتها ويمكن تلخيص هذه الأسباب فيما يلي:[2]

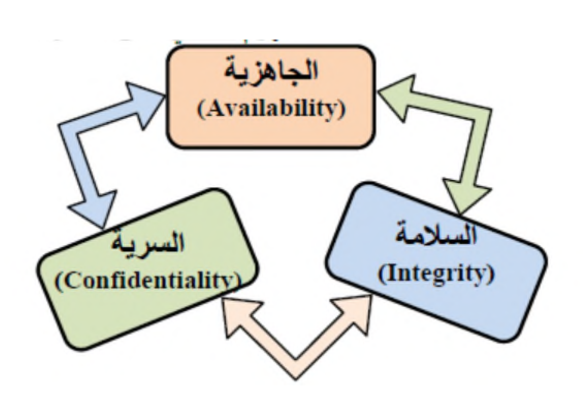
أولا: المحافظة على أمن المعلومات وحمايتها: إن الاعتماد التام والمتزايد على تكنولوجيا المعلومات والاتصال في المؤسسة نتج عنه أن جميع إجراءات أعمالها تتم آليا مما أدى إلى ظهور مخاطر ناتجة عن سوء استخدام تكنولوجيا المعلومات، فمنها مخاطر ناتجة عن مسائل تقنية بحتة تقع تحت مسؤولية إدارة تكنولوجيا المعلومات ومنها مخاطر أدارية وإجرائية لا بد من تضافر لجهود لردعها والسيطرة عليها، ومنها مخاطر خارجية أغلبها ناتجة عن أشخاص هدفهم العبث واللهو، لذلك يتوجب على المؤسسة العمل على حماية هذه المعلومات من التخريب أو سوء الاستخدام وذلك بتحقيق مستوى مقبول من الأمن المعلوماتي وذلك لضمان استدامتها وهذا لن يتم دون التخطيط

[1] اسراء جبريل رشاد مرعي:"**الجرائم الالكترونية:الأهداف-الأسباب-طرق الجريمة ومعالجتها**"، منشورات المركز الديمقراطي العربي، أوت 2016، متاح على الرابط:https://democraticac.de/?p=35426 تاريخ الاطلاع: 2020/01/30

[2] فايزة جيجخ، سميرة فرحات:" **حوكمة تكنولوجيا المعلومات و دورها في الوقاية من الازمات**"، مجلة الاقتصاديات المالية البنكية وادارة الأعمال، جامعة بسكرة، العدد 01، 2016، ص 119.

المسبق والسليم ، وأمن المعلومات لا يعني فقط عدم كشف أية معلومة وجب إبقاؤها سرا بل هناك جوانب أخرى لأمن المعلومات، حيث أن مفهوم أمن المعلومات يشتمل على ثلاث مكونات أو جوانب على درجة واحدة من الأهمية وهي: [1]السرية، السلامة، الإتاحة أو الجاهزية، والشكل الموالي يوضح المفهوم الثلاثي لأمن المعلومات:

الشكل رقم (01):المفهوم الثلاثي لأمن المعلومات.



المصدر: عقل محمد عقل: **مقدمة في حوكمة تقنية المعلومات**، مكتبة الملك فهد الوطنية، المملكة العربية السعودية، الطبعة الأولى، 2011، ص12.

ثانيا: تزايد قيمة الاستثمارات في تكنولوجيا المعلومات: نظرا لأهمية المعلومات بالنسبة للمؤسسة فإنها تعمل على توفير متطلباتها الفنية والبشرية وتستثمر في ذلك ميزانيات ضخمة خصوصا في القطاعات التي تعتمد اعتمادا كليا على التقنية مثل شركات الاتصال وشركات الطيران والقطاعات الصناعية والخدمية، وحيث أن هذه الاستثمارات تتعاظم يوما بعد يوم فإنه من الواجب حمايتها وتوفير سياسات وآليات لإقرار ومراقبة مشاريعها ذات القيمة العالية، كما أن هناك حاجة ملحة لتوفير أسس علمية وتطبيقية لدعم اتخاذ القرار وتفسير القيمة التي سوف تضيفها هذه الاستثمارات التقنية على أعمال المؤسسة وكيف ستقوم بخدمة أهدافها الإستراتيجية.[2]

ثالثا: قيمة المعلومة الإستراتيجية: لقد تعاظمت قيمة المعلومات في العصر الحديث حيث أصبحت لها قيمة عالية أكبر من أي وقت مضى وعلى مستوى المؤسسة فإن المعلومات التي يتم رصدها

---

[1] عقل محمد عقل، **مقدمة في حوكمة تقنية المعلومات**، مكتبة الملك فهد الوطنية، المملكة العربية السعودية، الطبعة الأولى، 2011، ص25.

[2] عقل محمد عقل، مرجع سابق، ص 15.

وجمعها عن نشاط المؤسسة وأعمالها وكذا عملائها وكل المتعاملين معها، تقدم العديد من المنافع على المستوى الاستراتيجي للمؤسسة حيث تمكن المعلومات الإدارة من مراقبة كل صغيرة وكبيرة في المؤسسة وتقدم لمتخذ القرار الأرضية الخصبة للدراسة ورصد التوجهات للسلوك العام للأعمال والعملاء وكذا المنافسين، كما أن توفير المعلومات ذات الدقة والموثوقية في المؤسسة يعطيها قيمة أكبر.[1]

رابعا: الخسائر الناتجة عن توقف هيكلة المنظومة المعلوماتية للمؤسسة: إن من العناصر المهمة والتي تعد قاعدة أساسية من قواعد أمن المعلومات مسألة التوافر أي توفر بيانات المعلومات وجاهزيتها للخدمة في الأوقات المحددة وبالجودة المطلوبة، حيث غياب هذه القاعدة والذي ينتج عن توقف هيكلة المنظومة المعلوماتية للمنظمة سيتسبب في خسائر مادية ومعنوية للمؤسسة ناهيك عن تشويه سمعتها في السوق.

خامسا: فرص التجارة الالكترونية بأنواعها: مما ل شك فيه أن تنامي حجم التجارة الالكترونية بمظاهرها المختلفة يتطلب توفير منظومة معلوماتية للمؤسسة آمنة وذات فعالية وكفاءة تنال ثقة المتعاملين وتحقق عائد أعلى من الاستثمارات التي يتم ضخها في بناء هذه المنظومة المعلوماتية وعلى سبيل المثال القوائم البريدية والتي تعد من الممتلكات غير الملموسة والتي تقدم للمؤسسة قنوات جديدة لترويج المنتجات وللتواصل الفعال مع العملاء.[2]

المحور الثالث: أساليب حوكمة تكنولوجيا المعلومات للحد من الجريمة المعلوماتية.

مما لا شك فيه أن جودة وأمن المعلومات يلعب دورا هاما في حماية أصول المنشأة، حيث أن هناك العديد من المخاطر لأمن المعلومات مثل تشويه المواقع، وقرصنة الخادم، وتسرب البيانات، ولقد أصبحت جودة وأمن المعلومات مصدر قلق كبير في قطاع الأعمال ولذلك فإن الشركات بحاجة ماسة إلى أن تدرك الحاجة إلى تخصيص المزيد من الموارد لحماية أصول المعلومات.[3].

---

[1] ثائر أحمد سعدون السمان، مراد موسى عبد الجبوري:" **متطلبات حوكمة تقنيات المعلومات ودورها في تحسين جودة الخدمات. دراسة حالة في المديرية العامة لانتاج الطاقة الكهربائية، صلاح الدين**"، المجلة العربية للإدارة، مجلد36، العدد 01، 2016، ص130.

[2] عقل محمد عقل، مرجع سابق، ص 17.

[3] حامد طلبة أوهيبة، أمل عبد الفضيل عطية: " **دور المراجعة الداخلية في ظل حوكمة تكنولوجيا المعلومات لتفعيل جودة وأمن المعلومات المحاسبية الالكترونية:دراسة اختبارية**"،جامعة بنها، كلية المحاسبة، مصر، 2012، ص 17.

وهناك مجموعة من الآليات لحوكمة تكنولوجيا المعلومات والمستخدمة للحد من انتشار الجريمة المعلوماتية وسوء استخدام البيانات ونظم المعلومات يمكن إجمالها في العناصر التالية: [1]

- المعايير العالمية مثل الإيزو ISO و الكوبيت COBIT و ITIL
- و بعض القوانين المرتبطة بأمن المعلومات مثل: **FISP**، **FISMA**، **SOX**
- مجموعة من الأدوات والممارسات مثل: **SYS TRUST, CMM,CMM/CMMI,** **6SIGMA**.

أولا: معايير الإيزو: الإيزو كمصطلح هي اختصار International Organization For Standarization وهي مسمى المنظمة العالمية للمعايير، وهذه المنظمة تقوم بوضع مقاييس عالمية لنظام إدارة الجودة الشاملة في أي منظمة سواء كانت إنتاجية أم خدمية، وتشمل على الثنائي المتوافق **ISO9001,ISO9004** وفائدة هذه المنظمة إصدار دليل مرشد لتطبيق نظام الجودة.

فالإيزو (ISO) عبارة عن نظام متكامل، يتكون من مجموعة من المعايير، والمقاييس المتعلقة بنشاط المنظمات، والتي يتم وضعها من قبل المنظمة الدولية للمقاييس (المعايير) لتقوم بدورها بمنح شهادات لهذه المنظمات في ضوء مدى توفر هذه المعايير لديها.

تتضمن سلسلة الإيزو 9000 مجموعة متناغمة من مقاييس تأكيد الجودة العامة المطبقة على أي شركة سواء كانت كبيرة أو متوسطة أو صغيرة، ويمكن أن تستخدم مع أي نظام موجود وتساعد الشركة على تخفيض الكلفة الداخلية وزيادة الجودة والفعالية والإنتاجية وتكون بمثابة خطوة باتجاه الجودة الكلية وتحسينها المستمر، وفيما يلي أهم المعايير التي تتعلق بأمن المعلومات: [2]

1. الإيزو 27001 (ISO27001): هو عبارة عن تطوير، تنفيذ، تشغيل، مراقبة، مراجعة، محافظة على، وتحسين نظام أمن المعلومات موثق في المنظمة يهدف إلى إدارة فعالة ومستمرة للمخاطر توفر حماية مناسبة للمعلومات حسب أهميتها، وهذا المعيار جزء من مجموعة من المعايير

---

[1] W.V.Grembergen&Steven.De Haes,"**IT Governance Structures,Processes and Relational Mecanisms:Achieving IT Business Alignment in Major Belgian Financial Group**"Proceedings of The 38th Hawaii International conference on System Sciences (ICSS),2005,P.2

[2] رياض عيشوش، فواز واضح: "حوكمة تكنولوجيا المعلومات: ميزة إستراتيجية في ظل اقتصاد المعرفة"، مداخلة مقدمة فعاليات الملتقى الوطني حول: حوكمة الشركات كآلية للحد من الفساد المالي و الإداري، جامعة بسكرة، الأردن، 6/7 ماي 2012، ص 1-4.

تسمى عائلة " ISO/IEC27000" أو يطلق عليها معايير تقنية المعلومات-تقنيات الأمن-كود الممارسة الأفضل لإدارة أمن المعلومات.[1]

2. الإيزو 27002 : هذا المعيار هو أحد معايير المنظمة العالمية للمعايير ويهدف إلى إيجاد خطط ومبادئ أساسية لإنشاء وتنفيذ وصيانة وتطوير نظم إدارة أمن المعلومات في المنظمة ويتوافق مع جميع المنشآت حكومية كانت أو خاصة بحيث تقوم كل منشأة بدراسة المخاطر المتعلقة بأمن معلوماتها ومن ثم بناء نظام أمن معلوماتي يقلل من المخاطر وقابل للتطوير.[2]

3. الإيزو 154080: ويساعد هذا المعيار على التقييم والتحقق والتصديق على الضمانات الأمنية للمنتجات التكنولوجية وكذلك يمكن تقييم الأجهزة والبرمجيات لمكافحة تغيير المناخ في مختبرات معتمدة للتصديق.

4. الإيزو (ISO/IEC17799,2000):

يقدم هذا المعيار توصيات حول الممارسات الجيدة في مجال إدارة أمن المعلومات وتهدف تلك التوصيات إلى توفير الثقة في المعاملات التي تتم بين المنظمات، ويقسم هذا المعيار مجال الرقابة الداخلية على أمن المعلومات إلى عشر أبعاد تتضمن: سياسة الأمن، الأمن التنظيمي، تصنيف الأصول ورقابتها، أمن الأفراد، الأمن المادي والبيئي، إدارة الاتصالات، إدارة العمليات، رقابة الوصول إلى المعلومات، تطوير الأنظمة و صيانتها، إدارة استمرارية الأعمال والالتزام.[3]

5. الإيزو 13335: التقرير الفني رقم 13335 لسنة 1996-2001 الصادر عن اللجنة الفنية المشتركة التي أسستها كل من المنظمة الدولية للمواصفات القياسية واللجنة الالكترونية الفنية الدولية (ISO/IEC 13335,1996_2001) ، وينقسم هذا التقرير إلى خمسة أجزاء هي:[4]

[1] أسامة بن صادق الطيب: " أمن المعرفة"، جامعة الملك عبد العزيز، الإصدار الثاني، 2012، ص59.

[2] IT Governance Institute ,"**Aligning Cobit 4,1 ,ITIL V3 And ISO/IEC 27002 For Business Benefit**" , USA , 2008 , p 10.

[3] Wallace E.McGHee,"**Information Technology Governance:An Exploratory Study of The Impact of Organizational Information Technology Security Planning** ",Thesis Of Ph.D,Capella University ,March,2008,p60.

[4] Steven De Haes,"**The Impact of IT Governance Practices on Business/IT Alignment In The Belgian Financial Services Sector**",Thesis of Ph.D ., University Antwerpen Management School,2007,p56.

- إيزو 13335-1: وهو عبارة عن مفاهيم ونماذج لإدارة أمن المعلومات، ويهدف إلى عرض المفاهيم الأساسية والنماذج اللازمة للتعريف بإدارة أمن المعلومات.
- إيزو 13335-2: وهو عبارة عن توثيق للتقنيات لإدارة أمن المعلومات التخطيطية، صدر هذا الجزء عام 1997 ويهدف إلى شرح الأنشطة المختلفة المرتبطة بإدارة أمن المعلومات وتخطيطه، كما يعرف بالأدوار والمسؤوليات المرتبطة بهذه الأنشطة.
- إيزو 13335-3: هي أساليب لإدارة أمن المعلومات، صدر هذا الجزء عام 1997 ويهدف إلى التعريف بالأساليب التي يوصى باستخدامها لإدارة أمن المعلومات المطلوب توفيرها، واختيار الضوابط الملائمة وتطبيقها والحفاظ عليها.
- إيزو 13335-4: يشمل اختيار الضوابط، ويهدف إلى تقديم إرشادات في مجال اختيار الضوابط وخاصة في ظل إتباع أحد مداخل تحليل الخطر وهو مدخل معايير الأمن، سواء كان اختيار الضوابط يتم وفقا لنوع نظام المعلومات أو وفقا لمتطلبات أمن المعلومات، وبالتالي فإن هذا الجزء يعد مكملا للجزء الثالث.
- إيزو 13335-5: يشتمل على التوجيه الإداري لأمن الشبكات ويهدف إلى تقديم إرشادات في مجال اختيار الضوابط الملائمة لأنظمة المعلومات التي تتصل بشبكات خارجية واستخدامها.

5. الإيزو (ISO/IEC38500/2008): جاء الدليل الخاص بمعايير الإيزو الذي صدر بعنوان"حوكمة تكنولوجيا المعلومات" لتعزيز فعالية وكفاءة وقبول تكنولوجيا المعلومات داخل المنظمة من خلال:

- تقرير ثقة المساهمين(يشمل المساهمين والموظفين) وأنه إذا تم إتباع هذه المعايير فإنهم يملكون الثقة في نظام حوكمة تكنولوجيا المعلومات في منظمتهم.
- إعلام وتقديم الدليل للمديرين لحوكمة استخدام تكنولوجيا المعلومات.[1]

ثانيا: معيار الكوبيت COBIT.

تعتبر الأهداف الرقابية على تكنولوجيا المعلومات COBIT بمثابة ترجمة للضوابط الرقابية التي أصدرتها لجنة COSO ولكن من الناحية التقنية لنظم المعلومات والوسائل التكنولوجية المرتبطة بها والتي أصدرها معهد إدارة تكنولوجيا المعلومات (ITGI) في تقرير الأهداف الرقابية

[1] رياض عيشوش، فواز واضح: " حوكمة تكنولوجيا المعلومات: ميزة إستراتيجية في ظل اقتصاد المعرفة"، مرجع سابق، ص 07

لتكنولوجيا المعلومات وفقا لقانون ساربانيس- اوكسلي (SOX) بهدف التأكيد على وجود ضوابط رقابية فعالة على التقارير والبيانات المالية التي تصدرها المؤسسة، وقد تم تصميم الضوابط الرقابية لإطار عمل COBIT لدعم ثلاث مستويات إدارية:

1. الإدارة التنفيذية ومجلس الإدارة.
2. الإدارة التنفيذية وتكنولوجيا المعلومات.
3. مسؤولي الحوكمة والتأكيد والرقابة والأمن.

واهتم إطار COBIT 4.1 بالربط بين أهداف المؤسسة والبنية التحتية لتكنولوجيا المعلومات من خلال تقديم مجموعة من النماذج المختلفة والتي تقيس مستوى الانجاز في تحقيق أهداف المؤسسة من خلال تحديد المسؤوليات المرتبطة بعمليات تكنولوجيا المعلومات وتنقسم هذه النماذج إلى أربعة مجالات محددة هي:

1. التخطيط و التنظيم.
2. التسليم والدعم لتكنولوجيا النظم.
3. اقتناء وتشغيل النظم التكنولوجية .
4. المتابعة والتقييم.

ويعتبر إطار COBIT 4.1 من أهم الأطر الرقابية التي تسعى المؤسسات لتطبيقها وقد تم الاعتراف بها من قبل المعايير الدولية المختلفة بما في ذلك ITIL, CMMI, COSO, PRINCE2, PMBOK, TOGAF, ISO 2700 ، ويعمل إطار COBIT على دمج جميع الضوابط الرقابية لتكنولوجيا المعلومات تحت مظلة واحدة.

وفي افريل 2012 تم إصدار أحدث إصدارات الأطر الرقابية COBIT 5 والذي عزز مبادئ COBIT 4.1 وإدماجها مع اطر مخاطر تكنولوجيا المعلومات و الذي تم إعداده وفقا لكل من إطار ضمان تكنولوجيا المعلومات ITAF, ISACA وذلك بهدف إيجاد نموذج لأمن المعلومات التكنولوجية للمؤسسة.[1].

1. مفهوم الأهداف الرقابية على تكنولوجيا المعلومات COBIT5: يعد إطار عمل COBIT 5 أداة تستخدم للرقابة على تكنولوجيا المعلومات طور بواسطة معهد حوكمة تكنولوجيا المعلومات في الولايات المتحدة الأمريكية عام 1929 ويحدد إطار العمل هذا 34 هدف ذو مستوى عال

---

[1] ميرفت حسين السيد: "حوكمة تكنولوجيا المعلومات ونشاط المراجعة الداخلية"، مجلة الأولى في التدقيق، العدد الأول، جويلية 2018، ص 52.

للرقابة على عمليات تكنولوجيا المعلومات كما يزود مدققي الحسابات بمجموعة من القياسات والمؤشرات المقبولة للحصول على حوكمة جيدة تساعدهم في إبداء رأيهم في المؤسسة وكانت أول نشرة صدرت لـ كوبت عام 1996 تلاها النشرة الثانية عام 1998 ثم الثالثة عام 2000 والأخيرة عام 2005.

كما يعد COBIT إطار عمل لإدارة مخاطر تكنولوجيا المعلومات ويساعد المديرين والمدققين والمستخدمين على فهم أنظمة تكنولوجيا المعلومات التي تخص شركتهم وكذلك يساعد في تطوير نموذج الحوكمة ويرشد إلى اختيار مستوى الأمان والسيطرة الضرورية لحماية أصول الشركة بشكل كفء وفعال.

ويحدد إطار عمل كوبيت 34 عملية متعلقة بتكنولوجيا المعلومات قسمت إلى أربعة أبعاد هي: التخطيط والتنظيم، الامتلاك والتنفيذ، التوصيل والدعم، المتابعة والتقييم.[1].

ويمكن تعريف الإطار الرقابي COBIT 5 على أنها إطار رقابي شامل يساعد المؤسسة في تحقيق أقصى استفادة من نظم تكنولوجيا المعلومات مع الحفاظ على التوازن بين تحقيق الفوائد وتحسين مستوى المخاطر والاستخدام الأمثل للموارد المتاحة لنظم المعلومات من خلال دعم نظام شامل لحوكمة تكنولوجيا المعلومات على مستوى المؤسسة بأكملها ومع الأخذ في الاعتبار كافة المستخدمين للنظم المعلوماتية للمؤسسة داخليا وخارجيا.

2. المبادئ الخمسة لمعيار كوبت COBIT 5: هي خمسة مبادئ تتيح للمؤسسة وضع إطار عمل فعال لحوكمة تكنولوجيا المعلومات وإدارتها بالاعتماد على مجموعة شاملة تضم سبعة عناصر تمكين لتعظيم فوائد الاستثمار في المعلومات والتكنولوجيا واستخدامها لتحقيق أهداف أصحاب المصالح، وفيما يلي عرض لها:

- تلبية احتياجات أصحاب المصالح.
- التغطية الشاملة لعمليات البنك.
- تطبيق إطار عمل جيد ومتكامل.
- تطبيق منهجية شاملة.
- الفصل بين الحاكمية والإدارة.

[1] لطيف زيود، حسين علي، ريم محمد نصور: "**أثر تطبيق حوكمة تكنولوجيا المعلومات وفق إطار COBIT على جودة التقارير المالية -دراسة ميدانية في المصارف السورية-**"، مجلة جامعة البعث، المجلد 36، العدد 2، 2014، ص 217.

3. عناصر التمكين السبع لمعيار COBIT 5: هي 7 عناصر تمكين تؤثر بمفردها أو مجتمعة على تمكين عمليات معيار كوبت 5 وفيما يلي بيان بمضمونها:

- المبادئ والسياسات وأطر العمل.
- عمليات حاكمية وإدارة تكنولوجيا المعلومات.
- الهياكل التنظيمية.
- المعلومات والتقارير.
- الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات.
- المعارف والمهارات والخبرات.
- منظومة القيم والسلوكيات.[1]

ثالثا:معيار ITIL:

وهو اختصار لـ The **I**nformation **T**echnology **I**nfrastructure **L**ibrary ويسمى أيضا آيزو 20000، ويتكون من سلسلة من المطبوعات التي توفر إرشادات حول توفير خدمات تكنولوجيا المعلومات ذات الجودة العالية وتوضيح للعمليات والوسائل الضرورية لتدعيمه.[2]

رابعا: القوانين و اللوائح المتعلقة بأمن المعلومات.

لقد صدرت العديد من القوانين واللوائح الدولية التي تتعلق بحوكمة تكنولوجيا المعلومات ومن أهمها:[3]

- **قانون SOX:** Sarbanes_**Ox**ley Act صدر قانون ساربانيس- اوكسلي علم 2002 بعد ارتفاع الممارسات غير السليمة في الولايات المتحدة بما في ذلك شركة انرون وشركة ورلدكوم والغرض منه هو حماية المستثمرين عن طريق تحسين دقة وموثوقية نظام الإفصاح.
- **إطار لجنة COSO:** Committee **O**f **S**ponsoring **O**rganizations of the Traed way Commission

[1] **دليل حاكمية وإدارة المعلومات والتكنولوجيات المصاحبة لها**، البنك العربي الإسلامي الدولي، افريل 2017.

[2] Pauwels, E, (2006). **Change Governance Series-Making Sense of Regulation and Best Practices**, Copyright Serena Software, Inc, august.p 234

[3] حامد طلبة أوهيبة، أمل عبد الفضيل عطية ، مرجع سابق، ص24.

قدمت اللجنة إطارا يبدأ من عملية الضوابط الداخلية كما أنه يساعد على تحسين وسائل السيطرة على الشركات من خلال تقييم فعالية الضوابط الداخلية ويشتمل على خمس مكونات رئيسية:

- البيئة الرقابية .
- التقييم الذاتي للمخاطر.
- الأنشطة الرقابية.
- المعلومات والاتصالات.
- المتابعة.

ويمكن إطار اللجنة المراجعين الداخليين و مراجعي نظم المعلومات الاسترشاد بهيكل COSO لتقدير المخاطر النسبية (الضمنية) في نظم التجارة الالكترونية ومن ثم السماح للمراجعين الداخليين لتحديد وبيان أساليب الرقابة التي بموجبها يمكن خفض المخاطر المحتملة الناتجة من توظيف تطبيقات التجارة الالكترونية مثل:

- تحديد الضوابط الهامة للبنية التحتية لتكنولوجيا المعلومات.
- توفير المعلومات اللازمة لإعداد التقارير للإدارة العليا.

▪ قانون **FISMA**: **F**ederal **I**nformation **S**ecurty **M**anagement **A**ct و يعني قانون إدارة أمن المعلومات الفيدرالي وهو يشكل جزءا من قانون الحكومة الالكترونية للولايات المتحدة الأمريكية(القانون العام 107-347) الذي أصبح تشريعيا في عام 2002 ويحتوي على متطلبات الحكومة الأمريكية لتطوير وتوثيق وتنفيذ برنامج تكنولوجيا المعلومات ويوفر الأمن المعلوماتي وأنظمة المعلومات التي تدعم عمليات وموارد المؤسسات البحثية.

▪ قانون **FIPS**: The **F**ederal **I**nformation **P**rocessing **S**tandards ويعني معايير معالجة المعلومات الفدرالية، وهو عبارة عن مجموعة من المعايير المستخدمة في أنظمة الكمبيوتر قامت بتطويرها الحكومة الأمريكية لتستخدمها المؤسسات غير العسكرية.

خامسا: الأدوات و الممارسات المتعلقة بأمن المعلومات.

هناك العديد من الأدوات والممارسات التي تتعلق بأمن المعلومات التكنولوجية وفيما يلي عرض لأهمها.

1. معيار **6SIGMA**: بدأ ظهور مفهوم 6 سيجما منذ ثلاثة عقود كإستراتيجية تتوجه نحو جودة عمليات التصنيع ليمتد استخدامها وينتشر ليشمل كل المجالات صناعية كانت أم إنتاجية أو خدمية

وسيجما هو الحرف الثامن عشر في الأبجدية الإغريقية ورمزه (σ)[1]، وقد استخدم الإحصائيين هذا الرمز للدلالة على الانحراف المعياري، والانحراف المعياري طريقة إحصائية ومؤشر لوصف الانحراف أو التباين أو التشتت أو عدم التناسق في عملية معينة بالنسبة للأهداف المنشودة، وتعرف 6سيجما على أنها الفلسفة، والمقاييس، والمنهجية التي تزود المؤسسات بالأدوات اللازمة لتحقيق مستويات عالية من الأداء لكل من المنتج والخدمات التي تقدمها، و يشار إليها على أنها"طريقة منضبطة لجمع البيانات، والتحليل الإحصائي[2] لتحديد مصادر الأخطاء وسبل القضاء عليها، فمنهجية6سيجما هي عملية[3] أو إستراتيجية تمكن المنشآت من التحسن بصورة كبيرة فيما يخص عملياتها الأساسية وهيكلها من خلال تصميم ومراقبة أنشطة الأعمال اليومية بحيث يتم تقليل الفاقد واستهلاك المصادر (الوقت - الطاقات الذهنية - الطاقات المادية) وفي نفس الوقت تلبية احتياجات العميل وتحقيق القناعة لديه، ويدل مبدأ 6 سيجما على أن المنشأة تقدم خدمات أو سلعا خالية من العيوب تقريبا لأن نسبة العيوب في 6 سيجما حوالي 3.4 عيب لكل مليون فرصة[4]، أي أن نسبة كفاءة وفاعلية العمليات تصل إلى 99.99966 %.

وفي الأخير يمكننا القول أن "6سيجما" هو منهج انتهجته المنظمات في عملياتها الأساسية وهيا كلها، حيث يتم من خلاله مراقبة الأداء والأنشطة والأعمال اليومية؛ بهدف الوصول لدرجة متقدمة من درجات الجودة الشاملة يتم فيها تقليل الفاقد وتقليص فرص العيب، لذا يعتبر هذا المنهج أسلوباً علمياً متفرداً في مثل هذه الحالات لتلبية حاجة العميل، ففكرة 6 سيجما تكمن في أنه إذا كانت المؤسسة قادرة على قياس عدد العيوب الموجودة في عملية ما فإنها تستطيع بطريقة

---

[1] Ron Basu and Nevan Wright: **Quality Beyond Six Sigma**, Elsevier Science Ltd, Great Britain 2003, p 34.

[2] Graham Wilson: **Six Sigma and the Product Development Cycle**, Elsevier Butterworth-Heinemann, Great Britain, 2005, p16.

[3] Ehrlich, Betsi Harris :**Transactional Six Sigma and Lean Servicing : leveraging manufacturing concepts to achieve world class service**, CRC Press LLC, Florida, 2002, p 01.

[4] Theodore T. Allen: **Introduction to engineering statistics and six sigma: statistical quality control and design of experiments and systems**, Springer-Verlag London Limited, London, 2006, p 08.

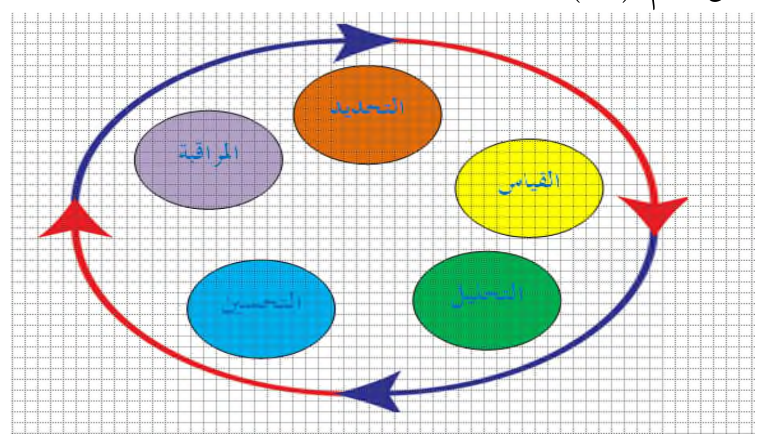
علمية أن تزيل تلك العيوب وتقترب من نقطة الخلو من العيوب، ويتطلب تنفيذ منهجية6 سيجما ما يلي:

1. تفادي التفرد في قيادة التطبيق واعتماد مبدأ القيادة الجماعية لأن تطبيق 6 sigma يعد من القرارات الإستراتيجية طويلة الأمد للمنظمة فضلا عن أنها تخص مخرجات المنظمة ككل.
2. ضرورة تحقيق التكامل والتنسيق في عمليتي التخطيط والتطبيق سواء على مستوى الإستراتيجية الشاملة أو على مستوى الإستراتيجية الوظيفية.
3. التركيز على التفكير العملي أثناء التطبيق وذلك لما تتميز به 6 sigma من أنها مدخل كمي يستخدم لمقارنة أداء المنظمة مع متطلبات الزبائن.
4. الاهتمام بتقليل الفجوة ما بين أداء المنظمة الفعلي المتمثل في جودة مخرجاتها ومنحنى متطلبات الزبائن.
5. القدرة على جمع وتحليل المعلومات الخاصة بمتطلبات الزبائن والسوق في آن واحد إذ لا بد من قياس مستوى الشعور بالرضا لديهم فضلا عن دراسة مدى شعورهم بالولاء لمنتجات المنظمة كما ولا بد من دراسة ومتابعة أداء المنظمات الأخرى بهدف تحقيق التميز على منتجاتها.
6. السعي لتحقيق عوائد على الاستثمار من خلال تعظيم الكفاءة والفعالية وتقليل نسب التلف باستخدام 6 sigma.
7. الاستعانة بدورات تدريبية لتطبيق أداة 6 sigma من خلال التواصل مع المنظمات الرائدة في تطبيق هذه الأداة.[1]
8. تهتم منهجية DMAIC بالتحديد والقياس والتحليل والتحسين والتحكم وتعتبر من أكثر النماذج شيوعا في تطبيق الـ 6 سيجما[2] وتستخدم هذه المنهجية لتحسين العملية القائمة والحد من العيوب في سيرها وتشتمل هذه المنهجية على خمس مراحل وهي:

[1] عبد الحميد عبد المجيد البلداوي، زينب شكري محمود نديم: "إدارة الجودة الشاملة و المعولية (الموثوقية) و التقنيات الحديثة في تطبيقها و استدامتها"، دار الشروق للنشر و التوزيع، عمان، الأردن، 2006، ص 107.

[2] L Ramanan, M Kumar: **SIX SIGMA - DMAIC Framework for Enhancing Quality in Engineering Educational Institutions,** International Journal of Business and Management Invention, Volume 3 Issue 1, January. 2014, p.36-40.

الشكل رقم (02) : منهجية **DMAIC لتطبيق مقياس ستة سيجما.**



Source: Gabriele Arcidiacono ; Claudio Calabrese ; Kai Yang: **Leading processes to lead companies: Lean Six Sigma, Kaizen Leader & Green Belt Handbook**, Springer-Verlag Italia 2012, p 02.

2. **CMM/CMMI:** هو نموذج نمو القدرات (CMM) وهو المنهجية المستخدمة لتطوير عملية البرمجيات في المنظمة أنشئ من قبل معهد هندسة البرمجيات (SEI) .

3. **خدمات الثقة TRUST SERVICES:** هي عملية منظمة لتجميع وتقييم الأدلة الكافية والملائمة بشأن تأكيدات الإدارة بخصوص فعالية تصميم وتشغيل النظام الالكتروني واختبار مدى توافق هذه التأكيدات مع مبادئ ومعايير قياس وتقييم الثقة في النظم الالكترونية التي أصدرها المعهد الأمريكي والكندي للمحاسبين القانونيين وتوصيل نتائج ذلك الاختبار إلى أصحاب المصلحة في تأكيد الثقة بالنظام الالكتروني.

وتعتبر شهادة SYS TRUST بمثابة تأكيد للثقة في نظام معلومات المنشأة بما يضمن سلامة وأمن إجراءات الرقابة الداخلية لنظام المعلومات، ويصدر المراجع تقريره يبين فيه مدى الاعتماد على هذا النظام في ضوء معايير ومبادئ خدمات الثقة، ومن أجل الوصول إلى تقرير نظيف يجب أن تتوافر المبادئ التالية:

- **التوافر:** بمعنى هل يتم تشغيل النظام بما يتفق مع متطلبات الأعمال المطلوبة من هذا النظام، هل النظام قابل للتشغيل والصيانة الروتينية.
- **الأمان:** بمعنى هل النظام تم حمايته ضد الدخول أو الاستخدام غير المصرح به للنظام.
- **الاكتمال:** بمعنى هل عمل النظام ومعلوماته تتسم بالكمال والدقة وأنه يستخدم في التوقيت المناسب وبالتطابق مع ما هو مصرح به.

- **القابلية للصيانة:** أن يتم تحديث النظام وتجديده عندما يتطلب الأمر ذلك بطريقة تسمح بتوافره بصفة مستمرة للمستخدم وبالأمان والنزاهة والدقة المطلوبة. [1].

خاتمة:

لقد واجهت منظمات الأعمال في مختلف القطاعات والأنشطة تحديات كبيرة فرضت عليها ضرورة استخدام التقنيات الحديثة والتكنولوجيا المتقدمة، إذ أصبح ذلك معيارا هاما في تطور هذه المنظمات ودافعا للتعامل معها والتنافسية في مجالات أعمالها، وقد تطلب ذلك قيام تلك المنظمات بإنفاق أموال ضخمة على الاستثمار في تكنولوجيا المعلومات وأنظمتها، غير أن هذه الاستثمارات الضخمة والتقنيات المعاصرة واجهت العديد من المخاطر والتهديدات والتحديات التي صاحبتها تحت مسمى "الجريمة المعلوماتية" إذ أفرزت البيئة الجديدة العديد من المتغيرات التي لم تكن موجودة من قبل في ظل استخدام الأساليب التقليدية في منظمات الأعمال مما استوجب استحداث آليات وأدوات لمواجهة هذا الجيل الجديد من المخاطر وتبين من خلال هذه الدراسة أن حوكمة تقنية المعلومات هي الحل الجوهري القابل للتطبيق من أجل تخفيض حدة المشكل باعتبارها العملية التي تصف المنظمات أو الحكومات التي تتبنى آلية فعالة وآمنة لتطبيق تقنية المعلومات التي يمكن أن تنجز المهام وتوازن المخاطر في عملية تطوير واستخدام المعلومات وتضمن أن تلك المنظمات يمكن أن تحقق أهدافا إستراتيجية من خلالها وأهمها:

- تسهيل تحقيق أهداف الإدارة من استخدام تكنولوجيا المعلومات والاستثمار فيها دون التعرض لمخاطر الجريمة المعلوماتية.
- دعم أعمال المؤسسة بما يزيد من الأرباح ويضغط النفقات.
- قياس أداء تكنولوجيا المعلومات في المؤسسة والتعرف على أهم مناطق وفرص التحسين للاستفادة منها.
- بناء ميزة تنافسية مستمرة للمؤسسة.
- توفير رابط قابل للقياس بين أهداف المؤسسة وأهداف الاستثمار في تكنولوجيا المعلومات.
- فتح آفاق جديدة للتوسع الأفقي والعمودي للمؤسسة.
- حماية استثمارات المؤسسة من كل الجرائم تقليدية كانت أومعلوماتية.

---

[1] ماجدة حسين ابراهيم: "تطوير أساليب الرقابة في مجال التجارة الالكترونية"، مجلة الفكر المحاسبي، كلية التجارة، جامعة عين شمس، العدد 02، 2005، ص 224.

- تقليل والتحكم في مخاطر تكنولوجيا المعلومات.
- دعم استمرارية الأعمال في كل الظروف.

التوصيات:

وفي ظل المعطيات السابقة الذكر ارتأينا تقديم مجموعة من التوصيات التي قد تساهم من الحد من الجريمة المعلوماتية وسوء استخدام النظم المعلوماتية على مستوى الوحدات الاقتصادية والمتمثلة أساسا في استحداث وحدات متخصصة لحمايتها وضمان أمنها وحسن استغلالها و يكون دورها الأساسي متمثلا في:

- إجراء تقييم دوري للمخاطر المرتبطة بأمن المعلومات ونظم المعلومات المستخدمة كالدخول غير المرخص به والإفشاء والتدمير والتعديلات وغيرها من المخاطر.
- وضع الأدلة والإجراءات والسياسات التي تتبع في تقييم المخاطر وزيادة العائد من الاستثمارات في تقنية المعلومات وتخفيض المخاطر المرتبطة بأمن المعلومات إلى المستويات المقبولة.
- التأكد من توافر إجراءات آمنة للمعلومات في كل مرحلة من مراحل نظم المعلومات بالمؤسسة بشكل عام.
- التأكد من توفر متطلبات أمن وحماية المعلومات طبقا لما تقرره الإدارة العليا ومجالس الإدارة والتشريعات والجهات الإشرافية وكذلك الترتيبات التعاقدية.
- تقديم المساندة والدعم من حيث تأمين المعلومات للشبكات والمرافق ونظم المعلومات والمجموعات المختلفة من مستخدميها.
- تدريب العاملين وكذلك موردي الخدمات للمؤسسة وكل من يستخدم نظم المعلومات وتنمية معارفهم فيما يتعلق بأمن المعلومات وإعلامهم بالمخاطر المرتبطة بأنشطتهم ويتعلق بأمن المعلومات وكذلك مسؤولياتهم طبقا لما تحدده سياسات وإجراءات العمل الموضوعة بالمؤسسة لتقليل المخاطر إلى أدنى حد ممكن.
- الفحص والاختبارات الدورية لمدى فعالية سياسات أمن المعلومات وإجراءاتها والممارسات العملية لها بواقع مرة على الأقل سنويا.
- إيجاد آلية لمتابعة ما تم اتخاذه من إجراءات لمعالجة أية ثغرات في سياسات وإجراءات أمن المعلومات وممارساتها العملية.

- إبلاغ الجهات المسؤولة بالمؤسسة أو جهات الإشراف والرقابة أو الجهات المحددة قانونا عن الأحداث الطارئة التي تؤثر على أمن ونظم المعلومات لديها ووضع النظم والإجراءات التي تكفل الاكتشاف المبكر لهذه الأحداث والتعامل معها لتخفيض مستوى المخاطر قبل وقوع الضرر.

دور التدقيق الداخلي في الحد من مخاطر الجريمة الالكترونية- دراسة ميدانية -

The Role of Internal Audit in Reducing Risks of electronic crime

د. زياني عبد الحق أستاذ محاضر أ.
جامعة ابن خلدون تيارت -الجزائر

1. مقدمة:

مما لاشك فيه أن العالم اليوم على أعتاب الثورة الصناعية الرابعة في تاريخ البشرية المستندة إلى الثورة الرقمية، التي تمثل اتجاها جديدا تصبح فيه التكنولوجيا جزءا لا يتجزأ من المجتمعات. وتتميز الثورة الصناعية الرابعة باختراق التكنولوجيا الناشئة في عدد من المجالات، بما في ذلك الروبوتات، الذكاء الاصطناعي و الحوسبة العمومية.

فهي تعتمد على التكنولوجيا والتقليل من التدخل البشري، بحيث يقتصر الدور البشري في الصناعة على المراقبة والتدقيق الداخلي، إلا أنه مقابل الإيجابيات الكبيرة التي يمكن أن تحققها هذه الثورة، فإن هناك سلبيات ستترتب عليها وستعاني منها المؤسسات الاقتصادية، بما فيها المؤسسات الكبيرة وخصوصا زيادة مخاطر الجريمة الإلكترونية.

ومن اجل هذا ظهرت جاءت وظيفة التدقيق الداخلي كأحد أهم الآليات الرقابية التي تهدف إلى التقليل من تلك المخاطر.

والتدقيق الداخلي يعتبر بمثابة وظيفة تقييمية يقوم بها شخص مهني محترف (موظف داخل المنشأة) من أجل الحصول على أدلة تتعلق بالأنشطة الاقتصادية بهدف تحديد مدي اتساق هذه الأنشطة بالمعايير الدولية للتدقيق الداخلي ومبادئ المحاسبة.

ومن خلال ما سبق يمكننا طرح الإشكالية التالية:

كيف يمكن للتدقيق الداخلي الحد من مخاطر الجريمة الالكترونية؟

2. أهداف الدراسة :

يهدف هذا البحث إلى التعرف على دور التدقيق الداخلي في الحد من مخاطر الجريمة الالكترونية ،من خلال دراسة نظرية ، وذلك من خلال التعرف على الإجراءات المضادة التي يلتزم بها المدقق الداخلي في الحد من مخاطر الجريمة الالكترونية.

3. منهج الدراسة :

اعتمد هذا البحث على المنهج الوصفي وذلك من خلال الكتب العلمية والمراجع والأبحاث لدراسة دور التدقيق الداخلي في الحد من مخاطر الجريمة الالكترونية، ومن ثم استخلاص النتائج وتقديم التوصيات التي تسهم في تطوير وظيفة التدقيق الداخلي والرفع من كفاءة وفعالية نظام الرقابة الداخلية.

4. الإطار المفاهيمي للتدقيق الداخلي والجريمة الالكترونية:

يعود أصل كلمة التدقيق إلى اللغة اللاتينية Audire والتي تعني السمع ،بالإضافة إلى أن كلمة التدقيق في اللغة الإنجليزية (to Audit) يقصد به الفحص والرقابة[1] ، والتدقيق يعتبر من أقدم المهن إذ أن الفراعنة في مصر و الإمبراطوريات القديمة في بابل واليونان كانت تحقق من صحة الحسابات عن طريق الاستماع إلى المدقق في الساحات العامة حول الإيرادات والمصروفات[2].

اما بالنسبة للتدقيق الداخلي فقد بدأت بوادره سنة 1941 نتيجة إنشاء المعهد الأميركي للمدققين الداخلين (Institute of InternalAuditing) بالإضافة إلى تقرير لجنة تريداوي (Treadway) هذه اللجنة التي جاءت لدراسة أسباب الاحتيال في التقارير المالية.

تحضا وظيفة التدقيق الداخلي بأهمية بالغة في وقتنا الحالي، نظرا للدور الذي تلعبه في الحد من عمليات الغش والاحتيال خاصة منها ما تعلق بالجرائم الالكترونية، وأصبحت كأداة لفحص وتقييم مدى فاعلية الأساليب الرقابية ومد الإدارة العليا بالمعلومات الكافية والموثوق منها وبهذا يصبح التدقيق الداخلي أداة تبادل للمعلومات والاتصال بين المستويات الإدارية المختلفة والإدارة العليا.

4.1 مفهوم التدقيق الداخلي:

لقد وردت العديد من التعاريف المختلفة للتدقيق الداخلي، إذ عرفه Robert Moellerعلى انه "وظيفة تقييمية مستقلة تم إنشاؤها داخل المنظمة من اجل فحص وتقييم أنشطتها خدمة للمنظمة."[3]

---

[1]. Mikol A., (2000), “ forme d’audit : L’audit interne » Encyclopédie de Comptabilité, Contrôle de Gestion et Audit”, Economica, Paris. p. 733.

[2].Lee Teck, H., & Azham, M. (2008). The Evolution of Auditing: An Analysis of the Historical Development. Journal of Modern Auditing and Accounting , 4, 2.

[3].Moeller , R. (2016). Brink's Modern Internal Auditing: A Common Body of Knowledge. New Jersey: John Wiley & Sons.p. 03

إلى أن التدقيق الداخلي هو عبارة عن «وظيفة عالمية تطبق في جميع Jaques Renardبينما يشير المؤسسات وعلى جميع الوظائف الممارسة على مستواها"[1]

ويرى أندرسون وآخرون أن التعريف الشامل للتدقيق الداخلي والذي يشتمل على الدور الحديث الذي أسند للمدقق الداخلي هو التعريف الذي قدمه المعهد الأمريكي للمدققين الداخليين، حيث أشار فيه هذا الأخير إلى أن التدقيق الداخلي عبارة عن: " نشاط مستقل وموضوعي، يقدم تأكيدات وخدمات استشارية بهدف إضافة قيمة للمؤسسة وتحسين عملياتها، ويساعد هذا النشاط في تحقيق أهداف المؤسسة من خلال إتباع أسلوب منهجي منظم لتقييم وتحسين فاعلية عمليات الحوكمة وإدارة المخاطر والرقابة"[2]

ومن خلال استعراض التعريفات السابقة نجد أنها اتفقت على مجموعة من النقاط الجوهرية والمتمثلة في :

- التدقيق الداخلي وظيفة مستقلة داخل المنشاة؛
- التدقيق الداخلي أداة رقابية تهدف إلى تقييم أنشطة المنظمة من خلال إصدار حكم انتقادي بخصوص هذه الأنشطة؛
- يهدف التدقيق الداخلي إلى خدمة المنظمة ومساعدتها في تحقيق أهدافها.

بينما يرى بعض الباحثين أن التعريف الاخير للتدقيق الداخلي يرتكز على خمسة عناصر أساسية والتي يمكن إستخلاصها فا يلي:

- مساعدة المنظمة حتى تحقق أهدافها؛
- تقييم وتحسين كفاءة العمليات الإدارية ،المخاطر والرقابة والحوكمة؛
- التأمين والأنشطة الاستشارية الهادفة إلى خلق القيمة، بالاضافة إلى تحسين عمليات المنظمة.
- الاستقلالية والموضوعية؛

---

1. Renard, J. (2013). Théorie et Pratique de l'Audit Interne. Paris: Eyrolles, p.28

2. Anderson , U., Head, M., Ramamoorti, S., Riddle, C., Salamasick, M., & Sobel, P. (2017). Internal Auditing: Assurance & Advisory Services. Greenwood: Internal Audit Foundation.p.30

- منهج منظم والمنهجي (عملية التدقيق).[1]

4.2 أهداف التدقيق الداخلي :

إن الهدف الأساسي للتدقيق الداخلي يكمن في المساهمة في خلق القيمة وهذا من خلال الدور الذي يقوم به المدقق الداخلي في الحفاظ على استمرارية المنشاة باعتباره شريك استراتيجي لها.

كما أن هناك أهداف أخرى لا تقل أهمية عن الهدف الأساس يشير إليها Spencer Pickettفي كتابه المعنون ب The internalauditingHandbook و المتمثلة فما يلي :[2]

- تعزيز الأخلاق والقيم المناسبة داخل المنظمة ؛
- ضمان إدارة الأداء التنظيمي الفعال والمساءلة ؛
- توصيل المعلومات المتعلقة بالمخاطر والرقابة إلى المناطق المناسبة في المنظمة وتنسيق الأنشطة بالإضافة إلى إيصال المعلومات إلى كل من المجلس، التدقيق الخارجي والداخلي والإدارة.

4.3 أنواع التدقيق :

هناك عدة أنواع قدمت للتدقيق بصفة عامة إلا أننا سوف نركز على التصنيف الحديث الذي جاء بيه كل من Brenda Porter et Alفي كتابه المعنون ب Pricnciples of ExternalAuditing ، حيث يري هذا الأخير ان التدقيق ينقسم إلى ثلاثة أنواع رئيسية:[3]

- تدقيق القوائم المالية (Financial Statements Audit)

وهو التدقيق الخارجي، حيث يكون الهدف منه هو الخروج برأي فني محايد عن مدى عدالة البيانات المالية و حقيقية تمثيلها للمركز المالي و نتيجة الاعمال والتدفقات النقدية وللمعايير المحاسبية. وهذا الرأي يكون بمثابة تأكيد معقول وليس مطلق عن مدى خلو البيانات المالية من الانحرافات المادية ، ويقوم المدقق بالتأكد من مدى مسايرة البيانات المالية لمعايير المحاسبة الدولية

[1]. Kurt F. Reding etAl, (2015), " Manuel D'audit Interne: Améliorer L'efficacité de la Gouvernance, du Contrôle interne et du Management des Risques", Eyrolles, Paris, p.4

[2]. Pickett, K.H. Spencer (2010), " The Internal auditing Handbook", Wiley, Third Edition, United Kingdom, p136.

[3].Brenda Porter et Al.,(2014), "Principles of Extrenal Auditing", Fourth Edition, John Wiley & Sons.Ltd, USA, p.4-5-6.

و في النهاية يقدم تقريره إلى المساهمين في الشركات المساهمة العامة والخاصة والتوصية بالأسهم وذات المسؤولية المحدودة والى من قام بتعينه في الشركات والمشاريع الأخرى.

- تدقيق الالتزام أو الإذعان: (Compliance Audit)

هذا النوع من التدقيق يتعلق بالحصول على أدلة تدقيقية من أجل تحديد مدى إذعان بعض الأنشطة المالية والتشغيلية للقوانين والقواعد والشروط المحددة ذات علاقة، وهذه القواعد أو القوانين أو الشروط قد يكون مصدرها الإدارة أو الدائنون او الحكومة وعادة توجه تقارير التدقيق في هذه الحالة إلى الجهة التي وضعت القواعد أو الشروط وقد يشمل التقرير على ملخص بالاستنتاجات ومدى الالتزام بالقواعد أو الشروط.

- التدقيق التشغيلي : (Operational Audit)

هذا النوع من التدقيق يتضمن الحصول على أدلة تتعلق بالأنشطة التشغيلية للمنشاة وتقيمها من أجل الحكم على كفاءة وفعالية هذه الأنشطة مقارنة مع الأهداف المحددة ، ثم تقديم توصيات التي يراها المدقق ضرورية ، ويطلق على هذا النوع أحيانا التدقيق الإداري أو التدقيق الأداء. وهذا النوع من التدقيق يقع تحت اختصاص المدققين الداخلين ، فهو يعتبر بشكل أساس من أقسام التدقيق الداخلي.

5. الجريمة الالكترونية:

تعتبر الجريمة الالكترونية من الجرائم الحديثة التي بدأت في الانتشار بشكل واسع في الآونة الأخيرة ، فقد عرفها البعض على أنها كل فعل إجرامي يستخدم الكومبيوتر في ارتكابه كأداة رئيسية. وقد ظهر اختلاف في تسميتها فهناك من سماها جرائم الكومبيوتر وجرائم الالكترونية وهذا المصطلح الأكثر شيوعا، والبعض الأخر أطلق عليها تسمية جرائم المعلوماتية. ويتميز مجرم الجريمة الالكترونية عن المجرم العادي بأنه متخصص و له القدرة الفائقة والمهارة التقنية.

وقبل التطرق إلى مفهوم الجريمة الالكترونية يجب عرض مفهوم الجريمة بصفة عامة أو ما يعرف بالجريمة التقليدية ، حيث يرى محمد نجيب أن الجريمة التقليدية هي " فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة، و تدبيرا احترازيا"[1]

---

9 - محمود نجيب حسني، (1989) شرح قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة ، ص 104

أما بالنسبة للجريمة الالكترونية فقد عرفها أحمد خليفة على أنها "ليست هي التي يكون النظام المعلوماتي أداة ارتكابها، بل هي التي تقع عليه أو في نطاقه"[1]

بينما يشير Rosenblatt أن الجريمة الالكترونية تعتبر بمثابة "نشاط غير مشروع موجه لنسخ أو حذف او الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه"[2]

في حين عّرفها أيضا مكتب المحاسبة العامة في الولايات المتحدة الأمريكية «G.O.A» بأنها" الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة، وإساءة استخدام المخرجات، إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدًا من الناحية التقنية مثل تعديل الحاسوب"[3]

من خلال ما سبق نلاحظ أن هذه التعاريف ترتكز أساسا على موضوع الجريمة، إلا أن هناك بعض التعاريف التي ارتكزت إلى وسيلة ارتكاب الجريمة أي ان التركيز في هذه التعاريف ينصب على الوسيلة التي ترتكب بموجبها الجريمة و المتمثلة في استخدام الحاسوب، ومن أهم هذه التعاريف التعريف الذي قدمه John Frost ، حيث أشار هذا الأخير أن الجريمة الالكترونية هي : فعل إجرامي يستخدم الحاسوب في ارتكابه كأداة رئيسية"[4]

إلا أن التعريف الأكثر شمولا هو التعريف الذي قدم في مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين و الذي أشير فيه أن الجريمة الالكترونية هي " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي او شبكة حاسوبية تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في البيئة إلكترونية"[5]

و تميز الجريمة الالكترونية بعدة مزايا أهمها :

1- .احمد خليفة الملط،(2006)، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الثانية، ص 98 .

2- .هشام رستم، (1992)، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط – مصر، الطبعة، الأولى، ص 33

3. كامل السعيد، (1993)، " جرائم الكومبيوتر و الجرائم الأخرى في مجال التكنولوجيا، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 25-28 أكتوبر 1993، ص27

4. محمد الفيومي،(1991)، مقدمة في علم الحاسبات الإلكترونية والبرمجة بلغة بيسك، دار الفرقان، عمان، الطبعة الثالثة، ص 20

5. مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين، الذي عقد في فينا في الفترة الواقعة ما بين 10-17نيسان لعام 2000، مشار إليه عند: أسامةالمناعسة وجلال الزعبي وصايل الهواوشة، جرائمالحاسوب والإنترنت، دراسة تحليلية مقارنة، دار وائل للنشر- عمان، الطبعة الأولى 2001، ص 73 .

- استهداف للكيانات المعنوية ذات قيمة مادية او معنوية او معنوية ومادية؛
- التباعد الجغرافي بين مرتكب الجريمة والضحية؛
- انخفاض حجم المخاطرة؛
- سهولة ارتكاب الجريمة بعيدا عن أعين الرقابة الأمنية؛
- سرعة وجود تقدير معين لحجم الضرر الناتج عنها؛
- صعوبة تحديد المجرم ومعرفة مكانه نظرا لتفاوت الفئة العمرية لمرتكبي الجرائم الالكترونية؛
- قصور التشريعات و القوانين التي تدين هذا النوع من المجرمين ؛
- سهولة التخلص من الأدلة المدينة للمجرمين.

5.1 الأفعال التي تشكل جرائم الالكترونية (الانترنت):

حسب مكتب الأمم المتحدة للمخدرات والجريمة فإن الأفعال التي تشكل الجرائم الالكترونية يمكن تنظيمها في ثلاثة مجموعات وهي :[1]

أ. **الأفعال ضد السرية والنزاهة وتوافر بيانات الحاسب أو النظم.**

- الدخول غير المشروع لنظام الحاسوب؛
- الدخول غير المشروع، اعتراض أو الاستيلاء على بيانات الحاسوب؛
- إنتاج أو توزيع أو امتلاك لأدوات إساءة استعمال الحاسوب؛
- اختراق الخصوصية أو أساليب حماية البيانات.

ب.أفعال ذات صلة بالحاسوب لمصالح شخصية او مادية أو أذى

- الاحتيال المتعلق بالحاسوب أو التزوير؛
- جرائم الحاسوب ذات الصلة بالهوية؛
- حقوق الطبع والنشر أو جرائم العلامة التجارية ذات الصلة بالحاسوب؛
- إرسال أو السيطرة على إرسال البريد المزعج؛

1. ذياب موسى البيداني، (2014)، الجرائم الالكترونية: المفهوم والأسباب ، الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية خلال الفترة 4،2014/09/5، كلية العلوم الاستراتيجية، عمان/ الأردن، ص03

- الأعمال ذات الصلة بأجهزة الحاسوب الشخصية التي تسبب بالضرر
- الإغراء أو استمالة الأطفال المتعلق بالحاسوب.

ج. الأفعال ذات الصلة بمحتويات الحاسوب

- الأفعال ذات الصلة بالحاسوب التي تنطوي على خطاب الكراهية؛
- الإنتاج أو توزيع أو حيازة المواد الإباحية عن الأطفال المتعلقة بالحاسوب؛
- الأعمال ذات الصلة بأجهزة الكومبيوتر في دعم جرائم الإرهاب.

5.2 أصناف الجريمة الالكترونية: تتعدد أصناف الجريمة الالكترونية بتشعب هذه الجرائم وسرعة تطورها ، فمنهم من يصنفها بالرجوع إلى وسيلة ارتكاب الجريمة، أو دافع المجرم، أو على أساس محل الجريمة ، حيث يرى صغير يوسف أنه يمكن تقسيم هذه الجرائم إلى ثلاثة أقسام : [1]

5.2.1 الجرائم الواقعة على الأموال : في ظل التحول من المعاملات التجارية التقليدية إلى المعاملات التجارية الالكترونية، و انجر عنه من تطور في وسائل الدفع والوفاء، وفي خضم التداول المالي عبر الانترنت، أصبحت هذه المعاملات عرضة لشتى أنواع الجرائم ومن اهمها :

- السطو على أرقام بطاقات الائتمان والتحويل الالكتروني الغير مشروع؛
- القمار وغسيل الأموال عبر الانترنت؛
- جريمة السرقة و السطو على أموال البنوك؛
- تجارة المخدرات عبر الأنترنت.

5.2.2 الجرائم الواقعة على الأشخاص:

لقد أصبحت المعلومة المتعلقة بالأفراد متداولة بكثرة وهذا راجع لتطور شبكة الانترنت، مما جعلها عرضة لانتهاك والاستعمال من طرف المجرمين و من أهم هذه الجرائم ما يلي:

- جريمة التهديد والمضايقة والملاحقة؛
- انتحال الشخصية والتغرير والاستدراج؛
- صناعة ونشر الإباحة؛
- جرائم القذف والسب وتشويه السمعة.

5.2.3 الجرائم الواقعة على أمن الدولة:

1. صغير يوسف،(2003) الجريمة المرتكبة عبر الانترنت، رسالة ماجستير في القانون، كلية الحقوق والعلوم السياسية ، جامعة مولود معمري تيزي وزو، ص 43-58

يمكن تلخيص الجرائم الالكترونية التي تهدد أمن الدولة فما يلي:

- الجماعات الإرهابية : استغلت الكثير من الجماعات الإرهابية سرعة المعلومة عبر شبكة الانترنت بغرض نشر أفكارها التكفيرية وبالتالي تهديد أمن الدولة؛
- الجريمة المنظمة: و يقصد بها استغلال الجماعات الإجرامية شبكة الانترنت لتمرير مخططاتهم الإجرامية
- الجرائم الماسة بالأمن الفكري : وتعني التأثير على معتقدات وتقاليد المجتمع من خلال نشر أفكار تؤدي إلى الهزيمة الفكرية.
- جرائم التجسس الالكتروني: وهي من أخطر أنواع الجرائم التي تهدد أمن الدولة، حيث يقوم المجرمون باستغلال شبكة الانترنت لتجسس على الأشخاص او الدولة أو المنظمات أو الهيئات او المؤسسات المالية أو المالية (التجسس الاقتصادي).

6. علاقة التدقيق الداخلي بالجريمة الالكترونية:

يلعب التدقيق الداخلي دورا هاما في الحد من مخاطر الجريمة الالكترونية،فقد أكد المعهد الدولي لمدققين الداخليين العالمي (IIA) على هذا الدور من خلال التعريف الذي قدمته اللجنة العلمية للعمل التابعة لهذا المعهد، حيث أشارت فيه هذه الأخيرة أن التدقيق الداخلي هو : " نشاط مستقل و موضوعي يقدم تأكيدات وخدمات استشارية بهدف إضافة قيمة للمؤسسة وتحسين عملياتها، ويساعد هذا النشاط في تحقيق أهداف المؤسسة من خلال إتباع أسلوب منهجي منظم لتقييم و تحسين فعالية عمليات الحوكمة و إدارة المخاطر و الرقابة".[1]

هذا الدور الذي يلعبه التدقيق الداخلي في عملية تقيم إدارة المخاطر تم تنصيص عليه صراحة في المعيار 2120 من المعايير الدولية للممارسة المهنية للتدقيق الداخلي الصادرة عن معهد المدققين الداخلين العالمي (IIA) (نسخة 2017)[2]

[1]The Institute of Internal Auditors, Definition of Internal Audiing, Standards & Guidance,: https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Definition-of-Internal-Auditing.aspx

[2].The Institute of Internal Auditors, Internal Standards for the Professional Practice of Internal auditing (Standards): https://na.theiia.org/standards-guidance/Public%20Documents/IPPF-Standards-2017.pdf

المعيار 2120: يجب على نشاط التدقيق الداخلي تقييم فعالية عمليات إدارة المخاطر والمساهمة في تحسينها، بمعنى تحديد ما إذا كانت عمليات إدارة المخاطر فعالة هو حكم ناتج عن تقييم المدقق الداخلي بأن :

- أهداف المؤسسة تساند وتتفق مع مهمة المؤسسة؛
- المخاطر الهامة يتم تحديدها وتقييمها؛
- يتم اختيار الاستجابة المناسبة للمخاطر بحيث يكون مستوى المخاطر في انسجام مع قابلية المؤسسة للمخاطر؛
- يتم التقاط المعلومات المتعلقة بالمخاطر والابلاغ عنها في الوقت المناسب عبر المؤسسة، لتمكين الموظفين والإدارة ومجلس الإدارة من القيام بمسؤولياتهم.

كما أكدت المعايير الدولية للممارسة المهنية للتدقيق الداخلي (نسخة 2017) على ضرورة استخدام المدققين الداخليين لمعارفهم و خبراتهم و ميزاتهم الأخرى، مثل الاستقلالية والموضوعية في تقييم فعالية الضوابط الأساسية في المؤسسة و ذلك بغرض مساعدة الشركة على تحقيق أهدافها:

المعيار 1220.ت.1:[1] يجب على المدققين الداخليين أن يبذلوا العناية اللازمة في أعمالهم وذلك بالأخذ بعين الاعتبار العناصر التالية:

- مدى العمل اللازم لتحقيق أهداف المهمة؛
- درجة التعقيد أو الأهمية النسبية أو أهمية المسائل التي يتم تطبيق إجراءات التطمين عليها؛
- ملائمة و فعالية مسار الحوكمة و إدارة المخاطر و الرقابة؛
- احتمال حدوث أخطاء جسيمة أو الاحتيال أو عدم الامتثال؛
- تكلفة أعمال التطمين مقارنة بالمنافع الكاملة؛

6.1 طرق التدقيق الداخلي للحد من مخاطر الجريمة الالكترونية :

من المعلوم وكما تم الإشارة سابقا يعتبر الدقيق الداخلي من أهم الأدوات التي تساعد في الحد من مخاطر الجريمة الالكترونية، وحتى يكون هذا الدور أكثر فاعلية في المنشاة يجب أن يكون في إطار حوكمة جيدة لان التدقيق الداخلي يعتبر من أبين أهم الأدوات الرقابية لحوكمة الشركات ، حيث أشار Richard Chambers، المدير السابق لمعهد المدققين الداخلين أن للوصول إلى حوكمة

[1]. The Institute of Internal Auditors, Internal Standards for the Professional Practice of Internal auditing (Standards), Op-Cite, p 07.

جيدة يجب توفر عنصرين أساسين، أولا نظام رقابة داخلية فعالا وثانيا فعالية الإدارة الإستراتيجية للمخاطر.[1]

6.1.1 تقييم فعالية نظام الرقابة الداخلية:

يلعب التدقيق الداخلي دورا هام في تحسين وتقييم نظام الرقابة الداخلية، إذ يعتبر من أولى أهدافه. فحسب Gramling et Al ، حوكمة الشركات تتكون من أربعة عناصر أساسي:[2] - التدقيق الخارجي-لجنة التدقيق – مجلس الإدارة وأخيرا وظيفة التدقيق الداخلي، وهذه الأخيرة لها علاقة مع كل عنصر من هذه العناصر والتي تسمح لها بالتقييم الفعال لنظام الرقابة الداخلية.

وفي هذا السياق، ينص قانون ساربينز أوكسلي(SOX) في جويلية 2002 على ضرورة أن يلعب التدقيق الداخلي دور أساسي في عملية إعداد تقرير من طرف مجلس الإدارة فيما يتعلق بفعالية وكفاءة نظام الرقابة الداخلية داخل المؤسسة. زيادة على ذلك ، أكدت المعايير الدولية للتدقيق الداخلي (معيار 2130)[3] الخاص بالرقابة على ان " يجب على نشاط التدقيق الداخلي تقييم مدى كفاية وفعالية الضوابط الرقابية في التعامل مع مخاطر المؤسسة المتعلقة بالحوكمة و العمليات التشغيلية و أنظمة المعلومات".

ويؤكد Hayes et Al ، أن تقييم نظام الرقابة الداخلية يجب أن يشمل ثلاثة عناصر:[4]

- الحصول على معرفة عامة حول الرقابة الداخلية خاصة فيما يخص وثائق و ملفات الرقابة الداخلية؛

---

[1]. Ifaci., (2010), « Les challenges de l'audit interne : aujourd'hui et demain », Actes du petit-déjeunerdébat, Disponible sur le site : www.ifaci.com/dl.php?...Actes-petit-dej-richard-chambers-22-10-10- VF_1.pdf

[2].Gramling A. A., Maletta, M. J., Schneider A., Church, B.K., (2004), " Rôle of the internal audit function in Corporate Governance: A Synthesis of the extant Internal Auditing Literature and Direction for Future Research", The journal of Accounting Literature.

[3]. The Institute of Internal Auditors, Internal Standards for the Professional Practice of Internal auditing (Standards), Op-Cite, p 14.

[4]. Hayes R, Dassen R, Schilder A, Wlaalge P.,(2005), ' Principes of Auditing : An Introduction to International Standars on Auditting", 2nd Edition, Pearson Eduction Limited, England, p.273.

- تقييم أولي فيما يخص الرقابة الداخلية؛
- تقييم نهائي قائم على اختبارات فعالية الرقابة؛

و يشير Howard& Johnson، أن نتائج الدراسة التي قامت بها لجنة Treadway المعروفة باسم لجنة حماية التنظيمات الإدارية في الفترة الممتدة بين(1987-1997) و التي كان موضوعها يتعلق بشأن التقرير المالي الاحتيالي في المنظمات العامة الأمريكية، أشارت إلى أن الغش الذي يحدث في المنظمات يرجع إلى نقص (Johnson., 2000)[1]: - فعالية أنظمة الرقابة الداخلية.
- فعالية وظيفة التدقيق الداخلي (الاستقلال)- قوة استقلال مجلس الإدارة.

ومن هنا يمكن أن نستخلص أن استقلالية التدقيق الداخلي لها تأثير كبير على عمل التدقيق الداخلي، فكلما كان التدقيق الداخلي مستقل كلما كان دوره في تقييم نظام الرقابة الداخلية أكثر فاعلية.

6.1.2تحسين وتقييم فعالية عمليات إدارة المخاطر:

يلعب التدقيق الداخلي كذلك دورا مهم في تحسين فاعلية إدارة مخاطر الجريمة الالكترونية، حيث يرى Gramling& Myers أن وظيفة التدقيق الداخلي لها تأثير كبير على العناصر الخمسة المكونة لإدارة مخاطر المؤسسة. حيث تعطي تأكيد معقولا على عملية إدارة المخاطر، أن المخاطر يتم تقييمها بشكل صحيح، و أن عملية إدارة المخاطر قد تم تقييمها بشكل صحيح، و أن الإبلاغ عن المخاطر تم تحديده بشكل صحيح و أن الميزانية على إدارة المخاطر الرئيسية قد وضعت[2]

من جهة أخرى، يمكن للتدقيق الداخلي أن يوفر خدمات استشارية وهذا بهدف ، إدارة المخاطر و الحد من تأثيرها ، وعمليات الرقابة، ويعتمد التدقيق الداخلي عند تقديم خدمات استشارية على الموارد الداخلية والخارجية المتاحة للمجلس وعلى مدى نضج المنظمة[3].

7. الخلاصة :

---

[1]. Johnson, Howard J., (2000),"Corporate Accountability and Risk", Tone at the top, Published by Institute of Internal Auditors, Issue 6, April 2000, p.1.

[2]. Gramling A.A., Myers P.M., (2006), "Internal Auditing's Role in ERM", Internal Auditor, pp.52- 62.

[3]. Spencer Pickett K.H., (2005), "Auditing the Risk Management Process", John Wiley &Sons, Inc, New Jersey.p.93.

تأليف مجموعة من الباحثين

سمحت هذه الدراسة بإظهار دور التدقيق الداخلي في الحد من مخاطر الجريمة الالكترونية من خلال دراسة نظرية تناولنا فيها وظيفة التدقيق الداخي كأحدى أهم الأدوات الرقابية في إدارة المخاطر بالإضافة إلى الجريمة الالكترونية التي أتضحت انها تعد من الأنماط الإجرامية الجديدة التي فجرتها حديثا ثورة تقنية المعلومات والاتصالات عن بعد، والتي تميز بخصائص مختلفة تماما عن الجرائم التقليدية.

كما تم التطرق إلى دور التدقيق الداخلي في الحد من الجريمة الالكترونية وهذا بالتركيز على عنصرين هامين هما تقييم نظام الرقابة الداخلية وفعالية إدارة المخاطر ،لذلك، فقد توصلنا إلى مجموعة من النتائج الموجزة على النحو التالي:

- التدقيق الداخلي أداة أساسية لا يمكن الاستغناء عنها في إدراة مخاطر الجريمة الالكترونية؛
- إن التدقيق الداخلي مسؤول عن تقييم كافة وظائف المؤسسة بما فيها المحاسبة، وبالتالي فهو مسؤول عن سلامة الصحة المالية من الأخطاء والتحريفات والتلاعبات التي تتم في إطار الجريمة الالكترونية؛
- إن الجريمة الالكترونية أصبحت من بين اخطر أنواع الجرائم ، لهذا وجب على المنشاة الاهتمام أكثر بالتدقيق الداخلي وجعله شريك إستراتيجي للحد من هذه المخاطر؛

التوصيات:

بناء على النتائج التي توصلت إليها الدراسة فانه يمكن تقديم التوصيات التالية:

- سن قوانين وتشريعات رادعة لحالات الغش والاحتيال في إطار الجريمة الالكترونية؛
- ضرورة إرساء آليات تزيد من درجة استقلالية المدقق الداخلي بشكل يزيد دوره أكثر فعالية.

تأليف مجموعة من الباحثين



المحور الثامن

الجهود الوطنية و الدولية لمكافحة الجريمة المعلوماتية و الوقاية منها

الجهود الدولية لمكافحة الجريمة الالكترونية

International efforts to combat electronic crime

د. بن عمار نوال
دكتوراه في الديمغرافيا
جامعة باتنة

1. مقدمة:

شهد العقد الأخير من القرن العشرين وبدايات القرن الحادي والعشرين تقدما هائلا في مجال التكنولوجيا عامة وتكنولوجيا المعلومات والاتصالات خاصة وما زال ينمو حتى يومنا هذا ويتسارع بخطى واسعة وسريعة أكثر من الأمس وأفرز هذا العصر العديد من آليات تصنيع المعرفة والمزيد من الوسائل التكنولوجية الحديثة التي جعلت العالم قرية كونية صغيرة.

كما أن العصر الراهن يعرف بعصر الثورة والمعلوماتية والتكنولوجية كما يعرف بعصر التلاحم العضوي بين الحواسيب والعقل البشري فالحواسيب غزت كل مجالات النشاط الإنساني المعاصر، وعلى الرغم من المزايا التي تحققت وتحقق في مجال تقنية المعلومات على جميع الأصعدة وفي شتى ميادين الحياة المعاصرة فإن هذه الثورة التكنولوجية المتنامية رافقتها في المقابل جملا من الانعكاسات السلبية الخطيرة، جراء سوء استخدام هذه التقنية المتطورة والانحراف عن الأغراض المتوخاة منها فقادت إلى تفشي ظاهرة من الظواهر الإجرامية المستحدثة ألا وهي الجرائم المعلوماتية، التي لم تعد تقتصر على إقليم دولة واحدة بل تجاوزت حدود الدول وهي جرائم مبتكرة ومستحدثة تمثل إحدى صور الذكاء الإجرامي مما صعب من مهمة إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية كما كشف عن عدم قدرة قواعد الملاحقة الإجرامية التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أو على صعيد الملاحقة الجنائية الدولية.

ولحداثة ظاهرة الجرائم المعلوماتية اهتم الباحثون بالبحث عن تعريف ملائم لهذه الظاهرة لكن دون جدوى، وفي هذا الإطار تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين تعريفا جامعا لجريمة المعلوماتية بأنها:"جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة

حاسوبية أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية."

وتكتسي معالجة هذا النوع من الجرائم أهمية بالغة بالنظر إلى الإشكالات العملية التي تطرحها وارتباط ظهورها بتكنولوجيا الحاسوب والانترنت مما أسفر عن تميزها بمجموعة من الخصائص جعلتها، تختلف عن غيرها من الجرائم واستوجب ضرورة التعامل معها بما يتلاءم مع هذه الخصوصية ناهيك عن أن مرتكبيها يختلفون عادة عن المجرمين التقليديين باعتبارهم أشخاصا على مستوى عالي من العلم والمعرفة فالفاعل في الجرائم المعلوماتية أو ما يسمى بالمجرم المعلوماتي ليس شخصا عاديا، إنما هو شخص ذو مهارات تقنية عالية قادر على استخدام قدراته لتغيير المعلومات أو تقليد البرامج أو تحويل الحسابات عن طريق استعمال الحاسوب بشكل غير مشروع.

وإزاء ذلك كان لابد من تكاثف الجهود الدولية من أجل مكافحة هذا النوع المستحدث من الجرائم التي لم تعد تتمركز في دولة معينة ولا توجه لمجتمع بعينه بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات مستغلة التطور الكبير للوسائل التقنية الحديثة في الاتصالات والمواصلات، ولذلك لا بد من تعزيز التعاون الدولي واتخاذ التدابير الفعالة للحد من هذه الظاهرة والقضاء عليها ومعاقبة مرتكبيها.

وعليه ومما سبق نطرح الإشكالية التالية: ما هي الجريمة الالكترونية؟ وفيما تمثل الآليات والجهود الدولية في مجال مكافحة الإجرام السيبراني؟.

2. **أهمية الدراسة:** لقد ساهمت عدة أسباب وعوامل على جعل الجرائم الالكترونية ظاهرة بالغة الخطورة على أمن المجتمع الدولي بوجه عام والمجتمع الإسلامي خاصة، الأمر الذي أدى إلى أهمية التعاون الدولي للتصدي لهذه الظاهرة الخطيرة والبحث في الوسائل الوقائية لإجهاض هذا النوع من الجرائم قبل وقوعها، خاصة وأن الحاسوب والانترنت قد صارا وسائط عالمية للتعامل بين الدول والشركات والأشخاص ويمثلان حاليا البنية الأساسية لكل المرافق التي تدار بالحاسوب بحيث أصبح عدم التعامل معهما خروجا من الدائرة الدولية، ومن هنا تتبين أهمية التعرض للجرائم الالكترونية من ناحية مكافحتها دوليا، إذ أن احتمالات تعرض الأشخاص والمؤسسات أو حتى الحكومات لجريمة الكترونية صارت مرتفعة جدا، ودليل ذلك حجم الجرائم الالكترونية مقارنة بالجريمة التقليدية مما يقودنا إلى إدراك عمق تأثيرها السلبي على المجتمع وكذا ضرورة العمل على مكافحتها دوليا.

3. **المنهج المتبع:** من أجل الإجابة على التساؤل المطروح اعتمدنا على المنهج الوصفي التحليلي، والذي يتناسب مع موضوع الدراسة من خلال وصف الجرائم الالكترونية وتحليلها لتحديد خصائصها وأركانها وكذا إبراز الجهود الدولية للحد والتصدي لهذه الظاهرة.

4. **التأصيل المفاهيمي للدراسة:** تعتبر الجرائم الالكترونية أو ما يسمى **cyber crimes** من الظواهر الإجرامية التي تقرع أجراس الخطر لتنبه مجتمعنا عن حجم المخاطر والخسائر الناجمة عنها، وذلك باعتبارها من الجرائم الذكية التي تنشأ أو تحدث في بيئة الكترونية، يقترفها أشخاص من ذوي القدرات التقنية والفنية[1]، حيث أصبحت تهدد المجتمعات ككل نظرا لانتشارها الواسع في مختلف مناطق العالم[2]، هذا ما جعل الدول تحد لمواجهة هذه الظاهرة الإجرامية المستحدثة، فرغم اختلاف سبل المكافحة إلا أنها تسعى لتصدي هذه الجريمة.[3]

1.4 ماهية الجريمة الالكترونية: إن مسألة وضع تعريف للجريمة الالكترونية كانت محلا لاجتهادات الفقهاء، لذا ذهب الفقهاء في تعريف الجريمة الالكترونية مذاهب شتى ووضعوا تعريفات مختلفة، ويتراوح تعريف الجريمة الالكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية، وتعرف الجرائم الالكترونية على أنها:"الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال."[4]

وهناك من عرفها على أنها: "الجرائم ذات الطابع المادي التي تتمثل في كل سلوك غير قانوني من خلال استخدام الأجهزة الالكترونية ينتج منها حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة، وغالبا ما يكون هدف هذه الجرائم هو القرصنة من أجل السرقة وإتلاف المعلومات الموجودة في الأجهزة، ومن ثم ابتزاز الأشخاص باستخدام تلك المعلومات."

---

[1] عبابنة محمود أحمد، جرائم الحاسوب وأبعادها الدولية، ط1، دار الثقافة للنشر والتوزيع، عمان، 2009، ص33.

[2] مصطفى محمد موسى، الجهاز الالكتروني لمكافحة الجريمة، د ط، دار الكتب القانونية، مصر، 2006، ص115.

[3] عبد الله عبد الكريم عبد الله، الجرائم الالكترونية دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، ط1، منشورات الحلبي الحقوقية، بيروت، 2007، ص16

[4] دياب موسى البدانية، 'الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية'، ملتقى علمي بالمملكة الأردنية الهاشمية، 2014، ص2.

تأليف مجموعة من الباحثين

لقد تعددت تعاريف الجريمة الالكترونية فهناك من تناولها من الزاوية التقنية أو من الزاوية القانونية، وهناك من عرفها اعتمادا على وسيلة ارتكاب الجريمة، كما عرفها الأستاذ **جون فورستر** بأنها:" فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسة"، كما أن هناك جانب من الفقه لا يهتم بالوسيلة أو موضوع الجريمة المعلوماتية ويعرفها بوصفها مرتبطة بالمعرفة الفنية أو التقنية باستخدام الحاسب الآلي، ولذلك عرفت هذه الجريمة بأنه:" أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسوب"، وبذلك عرفها **هشام فريد رستم** بأنها:" أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبيها."[1]

تتكون الجريمة الالكترونية من مقطعين هما الجريمة والالكترونية، ويستخدم مصطلح الالكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات، أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون، والجرائم الالكترونية فهي: "المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة ويقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الانترنت."[2]

ومن التعريفات التي وضعها أنصار الاتجاه الضيق أن الجريمة المعلوماتية هي: "كل فعل مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازما من ناحية، وملاحقته من ناحية أخرى"، كما عرفها هذا الاتجاه بأنها: "هي التي تقع على جهاز الكمبيوتر أو داخل نظامه فقط"، أما أصحاب الاتجاه الموسع يعرف الجريمة المعلوماتية بأنها: "كل سلوك إجرامي يتم بمساعدة الكمبيوتر، أو هي ك جريمة تتم في محيط أجهزة الكمبيوتر."[3]

فقد جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فينا سنة 2000 تعريف الجريمة الالكترونية بأنها:" أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوبي، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية."[4]

---

[1] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، د.ط، دار الثقافة للنشر والتوزيع، الأردن، 2011، ص29.

[2] عادل يوسف عبد النبي البشكري، "الجريمة المعلوماتية وأزمة الشرعية الجزائية"، العدد السابع، الكوفة، د.س، ص113.

[3] دياب موسى البدانية، مرجع سابق، ص3.

[4] محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الالكترونية، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2014، ص118.

أما التعريف الدولي للجريمة الالكترونية فهو يعتمد في الغالب على الغرض من استخدام المصطلح:"فهناك عدد محدود من الأفعال التي تمس السرية والنزاهة، وبيانات الكمبيوتر وأنظمته تمثل جوهر الجريمة الالكترونية، كما أن هناك أعمال متعلقة بالكمبيوتر لتحقيق مكاسب شخصية أو مالية أو ضرر بما في ذلك الأفعال المتصلة بجرائم محتويات الكمبيوتر. "[1]

6. الجهود الدولية لمكافحة الجريمة الالكترونية: إن الأمم المتحدة وأغلب المنظمات الدولية تولي موضوع الجريمة المعلوماتية اهتمام خاصا، وهو الأمر الذي أفرز مجموعة من الاتفاقيات الدولية في هذا المجال، وفي هذا السياق نشير إلى أهم الاتفاقيات التي تتناول هذا النوع من الجرائم بهدف مكافحتها والحد منها.

1.6 مواجهة الجريمة الالكترونية على المستوى الدولي:

لقد بذلت جهود دولية عديدة لمكافحة الجريمة الالكترونية وكان لها دور فعال في إطار التصدي لهذا النوع المستحدث من الجرائم من جهة، وكيفية تصدي بعض التشريعات المقارنة لهذه الجريمة من جهة أخرى.

أولا/ مساعي بعض الأجهزة الدولية في مواجهة الجريمة الالكترونية: للمنظمات الدولية دور فعال في التصدي للجريمة الالكترونية، باعتبارها من الجرائم العالمية، التي يستوجب فيها التعاون الدولي لمكافحتها وتقتصر في بعض الأجهزة الدولية في مجال مواجهة هذا النوع المستحدث من الجرائم.

أ. دور الأمم المتحدة في مواجهة الجريمة الالكترونية: اهتمت الأمم المتحدة بموضوع الجريمة الالكترونية، ووضعته من بين أولويات نشاطها نظرا لما تسببه هذه الأخيرة من أضرار وخسائر فادحة، وتؤكد على أن منع هذه الجرائم يتطلب استجابة دولية مشتركة بين أعضاء هذه المنظمة بغية التعاون للحد من انتشارها وتعاظم نتائجها، من خلال إشرافها على العديد من المؤتمرات الدولية الخاصة لردع الجريمة ومعاقبة المجرمين وإبرامها للاتفاقيات الدولية.[2]

نجد من بين أهم المؤتمرات المبرمة في مجال مكافحة الجريمة الالكترونية، المؤتمر الثامن المنعقد سنة 1990 الذي توصل إلى عدة توصيات بعد دراسته للتقرير الذي أعدته لجنة الخبراء

[1] خالد عياد الحلبي، مرجع سابق، ص30.

[2] إيمان مسعود سالم، الجريمة المعلوماتية، مذكرة لنيل شهادة الماستر، كلية الحقوق، جامعة محمد لمين دباغين، سطيف، 2015، ص32.

العشرين، بتكليف من المؤتمر السابع المنعقد بميلانو سنة 1985 حول موضوع حماية نظم المعالجة الآلية والاعتداءات التي تمس الحاسوب الآلي.

أما فيما يخص الاتفاقيات نذكر على سبيل المثال:

- الاتفاقية المنشئة للمنظم العالمية للملكية الفكرية (**معاهدة الويبو**) في ستوكهولم 1967 ، والتي دخلت حيز التنفيذ سنة 1970، إذ تعتبر هذه المنظمة إحدى الوكالات المتخصصة للأمم المتحدة حيث قامت هذه المنظمة من خلال مجموعة عمل تضم عددا من الخبراء بالعديد من المساهمات بهدف حماية برامج الحاسب الآلي، وهو ما ذهبت إليه أغلب الدول الصناعية ودول العالم الثالث إلى إخضاع برامج الحاسب الآلي لقوانين حماية حق المؤلف، ومنذ ذلك قامت أغلب التشريعات بتعديل قوانينها الخاصة بحق المؤلف، وأضافت برامج الحاسب الآلي إلى المصنفات الأدبية المجمعة وفقا للقانون، وذلك في إطار اتفاقية التجارة العالمية "**GATT**"، بالتالي لعبت المنظمة العالمية للملكية الفكرية دور في حماية حقوق المؤلف وبرامج الحاسوب.

- اتفاقية **تريبس** هي الأخرى من المعاهدات التي تم إنجازها في مجال حماية الملكية الفكرية من السطو عليها خصوصا مع انتشار عمليات السطو الالكتروني على الأعمال الفنية، دون إعطاء مالكيها أي من حقوقهم المادية أو المعنوية.

وتلك الاتفاقية تم التوقيع عليها من قبل الدول الأعضاء بها عام 1994، وقد عالج موقعو الاتفاقية العامة للتعريفات والتجارة حقوق الملكية الفكرية بتوقيع اتفاق الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية فربطوا بذلك بين المعايير الدولية والمعايير المحلية.[1]

لقد تناولت اتفاقية تحرير التجارة العالمية مختلف مناحي النشاط التجاري على الصعيد الدولي ونظرا لأهمية حماية الملكية الفكرية في ظل نظام تجاري عالمي جديد، فقد جاءت اتفاقية تريبس لمفاوضات استمرت عدة سنوات لتكون واحدة من أهم أدوات تحرير التجارة العالمية والتي أثارت جدلا ونقاشا طويلا أثناء المفاوضات بين الدول النامية والدول الصناعية المتقدمة.[2]

شملت مواد اتفاقية تريبس الخاصة بأوجه التجارة المتصلة بحقوق الملكية الفكرية على مكافحة الجريمة المعلوماتية بالنص في المادة 1/10 على أنه تتمتع برامج الحاسب الآلي أو الكمبيوتر

---

[1] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005، ص201.

[2] رشا علي الدين، النظام القانوني لحماية البرمجيات، دار الجامعة الجديدة، الإسكندرية، 2007، ص173.

سواء كانت بلغة المصدر أو بلغة الآلة بالحماية باعتبارها أعمالا أدبية بموجب معاهدة برن 1971 كما نصت في فقرتها الثانية على حماية البيانات المجمعة أو المواد الأخرى بشروط معينة.

لفعالية هذه المكافحة اشترطت الاتفاقية على الدول الأعضاء لحماية حقوق الملكية المنصوص عليها في هذه الاتفاقية وبهدف تسهيلا اتخاذ تدابي فعالة ضد أي تعدي على حقوق الملكية الفكرية التي تناولتها الاتفاقية، يجب اتخاذ إجراءات سريعة لمنع التعديات والانتهاكات الحالة في المادة 41 من الاتفاقية، وضرورة توافر إجراءات قضائية ومدنية إلى جانب إجراءات إدارية أخرى في المادة 42 منها، هذا ونصت المادة التاسعة من الاتفاقية على أنه على الدول الأعضاء فيها الالتزام بأحكام المواد من 1 إلى 21 من معاهدة برن 1971، مع مراعاة أن الحماية تسري على المنتوج وليس على مجرد الأفكار أو الإجراءات أو أساليب العمل، نصت على الحماية الزمنية لهذه المصنفات وحددتها بطول حياة المؤلف بالإضافة إلى مدة خمسين عاما بعد وفاته.[1]

- الاتفاقية الخاصة بمكافحة جريمة إساءة استعمال التكنولوجيا لأغراض إجرامية رقم 55_63 التي أبرمت في 2000/04/12، حيث ركزت على المساهمات التي يمكن أن تقدمها الأمم المتحدة ولا سيما لجنة منع الجريمة وتحقيق العدالة الجنائية، والترويج لمزيد من الفعالية والكفاءة في تنفيذ القوانين وإقامة العدل، كما أكدت على ضرورة منع إساءة استعمال التكنولوجيا لأغراض إجرامية، والحاجة للتعاون وتعزيز التنسيق بين الدول والقطاع الخاص على مكافحة وردع هذه الجريمة.[2]

ب. دور المجلس الأوروبي في مواجهة الجريمة الالكترونية: للمجلس الأوروبي دور فعال في سبيل الحد من الجرائم المعلوماتية وذلك من خلال إقراره العديد من التوصيات الخاصة بحماية البيانات ذات الصبغة الشخصية من سوء الاستخدام، وحماية الدفق المعلوماتي ومن بين مجهودات الاتحاد الأوروبي بصدد مكافحة الجريمة الالكترونية تمثل فيما يلي:

- التوقيع على الاتفاقية الخاصة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات، والتي وقعت بين المجلس الأوروبي والسوق الاشتراكية وكان ذلك في 17 سبتمبر 1980، وقد بدأ السريان الفعلي لهذه الاتفاقية في أكتوبر 1985، ويقتصر نطاق تطبيقها على الأشخاص الطبيعيين ويسري

---

[1] طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2012، ص74.

[2] حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الانترنت، 2007، ص1-3، مقال منشور على الرابط الالكتروني التالي: http://www.minshawi.com

على القطاعين العام والخاص بشأن الملفات المعدة آليا، بحيث تقضى بإلزامية أحكامها لتحقيق حماية البيانات الشخصية للمعالجة آليا[1]، بالإضافة إلى ما صدر عن المجلس الأوروبي من توصيات، تؤكد على توسيع نطاق الحماية لتشمل قطاعات الأنشطة الخاصة مثل البيانات الطبية والإحصائية، وفي سنة 1989 قام المجلس الأوروبي بنشر دراسة تتضمن توصيات تبين أهمية تفعيل دور القانون في مواجهة الجرائم المرتكبة عبر الحاسب الآلي، كما استتبعت هذه التوصية بدراسة أخرى سنة 195 تمحور حول الإجراءات الجنائي المتعلقة بالجرائم المعلوماتية، ومحاولة المجلس الأوروبي لتطبيق ما جاء في هذه التوصيات فقد قام المجلس الأوروبي بتشكيل لجنة خبراء الجريمة عبر العالم الافتراضي سنة 1997، كما نجد أيضا أن المجلس الأوروبي قد وقع أيضا على اتفاقية بودابست لمكافحة الجرائم الالكترونية الموقعة في 2001/11/23 بالتعاون مع كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية، ولم تدخل حيز التنفيذ إلى غاية 2004 بالرغم من أنها أوروبية المنشأ إلا أنها ذات طابع دولي فهي تعتبر اتفاقية جنائية دولية وأداة لمكافحة الجريمة السيبرانية.[2]

ت.دور المنظمة الدولية للشرطة الجنائية في مواجهة الجريمة الالكترونية: تهدف المنظمة الدولية للشرطة الجنائية الانتربول، إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة[3]، وكذا مساهمتها في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف، حيث تركز اهتمام الانتربول في السنوات الأخيرة بصورة أساسية على الجريمة المنظمة والأنشطة ذات الصلة بها، وخير دليل على ذلك اختتام أعمال اجتماع الجمعية العامة ال26 للشرطة الجنائية الدولة "الانتربول" بالعاصمة الصينية بكين سنة 29-09-2017 بمشاركة نحو 1000 من كبار قادة الشرطة والسياسيين في 156 دولة، ومن بين أهم القضايا التي تم

---

[1] الحسيناوي علي جبار ، جرائم الحاسوب والانترنت، د.ط، البازوري العلمية للنشر والتوزيع، عمان، 2009، ص151.

[2] Haddad Fella, La cybercriminalité, mémoire de fin d'études pour l'obtention de master, option droit privé de sciences criminelles, faculté de droit et de science criminelles, Université Abderrahmane Mira, Bejaia, 2012, p2.

[3] بن عمر الحاج عيسى، "الانتربول ك آلية دولية شرطية لمكافحة الجريمة المنظمة العابرة للحدود"، مجلة الدراسات القانونية السياسية، العدد 03، كلية الحقوق، جامعة الأغواط، 2016، ص252.

مناقشتها ضمن الاجتماع نجد جرائم الانترنت والقرصنة الالكترونية والمخاطر الناجمة عنها، وآلية التصدي لهذا النوع من الجرائم على المستوى الدولي.[1]

يؤدي الانتربول دور رائد في مجال مكافحة الجريمة الالكترونية ويتجلى من خلال تشجيع التعاون بين أجهزة الشرطة في الدول الأطراف من أجل مكافحة هذا النوع من الإجرام، كما تقوم بتزويد دول الأعضاء بالبيانات والمعلومات المتعلقة بالمجرم والجريمة، وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنظمة إليها، بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف، حيث تقوم بملاحقة مجرمي المعلوماتية عن طريق تعقب الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابر للحدود للأنظمة المعلوماتية وشبكات الاتصال بحثا عن الأدلة وبراهين على ارتكاب الجريمة الالكترونية كلها أمور تستدعي القيام ببعض العمليات الشرطية والأمنية المشتركة وهي من شأنها متابعة المجرمين الذين يستغلون التكنولوجيا الجديدة لتحقيق أغراضهم غير الشرعية.[2]

وإذا ما أردنا تقييم دور منظمة الانتربول، فإنها تعتبر من أهم المنظمات الدولية الناجمة والفعالة في أداء مهامها على المستوى الدولي، بحيث ساهمت في تحقيق التعاون الدولي بين أجهزة الشرطة في بلدان الأعضاء، ويرجع هذا إلى كون المنظمة الدولية للشرطة الجنائية تختص بمكافحة الجريمة المنظمة بمختلف أشكالها ومن بينها جرائم الالكترونية، فهي تعتبر جهاز رئيسي لتحقيق التعاون الدولي في مكافحة الجريمة المنظمة.[3]

ت. **دور الجامعة العربية في مواجهة الجريمة الالكترونية:** إن التطور السريع لتكنولوجيا الإعلام والاتصال وتطبيقاتها جعلتنا نعيش في عالم افتراضي، حيث فتح مجالات عديدة للاستفادة منها مؤديا في ذات الوقت إلى زيادة الخروقات والتهديدات التي تمس بأمن الأشخاص والمؤسسات، فلم يعد أحد بأمن عن مخاطر الجرائم الالكترونية باختلاف أساليبها وصورها التي تتخذ المعلوماتية والانترنت مسرحا لها.

---

[1] شبلي مختار، الجهاز العالمي لمكافحة الجريمة المنظمة، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2016، ص266-267.

[2] شبلي مختار، مرجع ص274.

[3] شحادة يوسف، الضابطة العدلية علاقتها بالقضاء ودورها في سير العدالة الجزائية (دراسة مقارنة)، ط1، مؤسسة يحسون للنشر والتوزيع، بيروت، ص456-458.

مما دفع بالدول العربية إلى محاولة إيجاد طرق تشريعية ناجعة لمواجهة هذه الجرائم، ومن بين هذه الجهود نذكر القانون العربي الاسترشادي، حيث قامت جامعة الدول العربية من خلال الأمانة العامة لمجلس وزراء العدل العرب في دورته التاسعة عشر، باعتماد هذا القانون النموذجي بالقرار رقم 459-19 في 2003/10/08 والذي يعتبر أهم ما بذل من جهود عربية في مجال الحماية التشريعية من الجرائم المعلوماتية.

تضمن هذا القانون 27 مادة مقسمة إلى أربعة فصول، الباب الأول يتحدث عن الجرائم المعلوماتية من المواد 3 إلى 22 وأهم الجرائم التي تناولها:

أ. جريمة الدخول غير المشروع إلى الموقع أو النظام المعلوماتي مع تشديد العقوبة إذا كان الغرض من الدخول إما الإتلاف أو الإلغاء أو إلحاق الضرر.[1]

ب. جريمة تزوير المستندات المعالجة آليا ي النظام المعلوماتي واستعمالها.

ت. مختلف الجرائم المخلة بالآداب العامة المرتكبة عبر شبكة المعلومات.

أما الباب الثاني منه فقد تناول التجارة والمعاملات الالكترونية، بينما تناول الباب الثالث حماية حقوق المؤلف عبر الوسائل الالكترونية، أما الباب الرابع فتطرق للإجراءات المتعلقة بالجريمة المعلوماتية نجد أن كل من منظمة الأمم المتحدة والمجلس الأوروبي والمنظمة الدولية للشرطة الجنائية، والجامعة العربية قد ساهموا في مكافحة الجريمة الالكترونية، رغم اختلاف الأساليب المنتهجة لمكافحة هذه الجريمة، إلا أنها تسعى كلها إلى تحقيق نفس الهدف وهو التصدي لهذا النوع المستحدث من الجرائم.

ثانيا/ المكافحة الإجرائية للجريمة المعلوماتية في الاتفاقيات الدولية: لا غنى للقواعد الموضوعية عن القواعد القانونية الإجرائية، ذلك أنها تفقد قوتها النافذة بدونها، والقاعدة الإجرائية ليست غاية في حد ذاتها وإنما هي وسيلة لغاية تمثل في إحكام وحسن تطبيق القانون الجنائي الموضوعي.[2]

إن مكافحة الجريمة المعلوماتية من الناحية الإجرائية يظهر من خلال وضع واستحداث إجراءات للبحث والتحري عن الجريمة المعلوماتية وإجراءات أخرى للكشف عنها والإيقاف والقبض على مرتكبيها.

---

[1] إيمان مسعود سالم، الجريمة المعلوماتية، مذكرة لنيل شهادة الماستر، كلية الحقوق، جامعة محمد لمين دباغين، سطيف، 2015، ص37.

[2] علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دار المكتب الجامعي للحديث، الموصل، 2012، ص11.

- **مفهوم المكافحة الإجرائية:** عرف قانون الإجراءات الجزائية بأنه "القانون الذي ينظم وسائل التحقق من وقوع الجريمة ومحاكمة مرتكبيها وتوقيع الجزاء عليهم، وينظم المحاكمة الجنائية ويحدد درجاتها واختصاصاتها ويبين الإجراءات التي تتبع في تحقيق الجرائم ومحاكمة مرتكبيها وتوقيع العقوبات عليهم، وينظم سير الدعوى الجنائية التي ترفع أمام القاضي الجنائي كما أنه يضع القواعد الخاصة بالطعن في الأحكام الجنائية ويكفل دقة وسلامة هذه الأحكام.[1]

كما عرف قانون الإجراءات الجزائية أيضا على أنه: "مجموعة القواعد والأحكام التي تنظم تشكيل واختصاص الهيئات المختلفة، التي تتولى ضبط الجرائم وتحقيقها ورفع الدعوى بشأنها ومباشرتها والفصل فيها وقوة الأحكام الجنائية وآثارها وطرق الطعن فيها".[2]

عرف أيضا على أنه:" مجموعة قواعد قانونية تحدد السبل والقواعد المقررة للمطالبة بتطبيق القانون على الكل من أخل بنظام الجماعة بارتكابه للجريمة جناية أو جنحة أو مخالفة، ويحدد الأجهزة القضائية وشبه القضائية واختصاصاتها والإجراءات المتبعة في المراحل الإجرائية المختلفة التي تهدف جميعها إلى الوصول للحقيقة المنشودة المتمثلة في تطبيق القانون على من خرقه، عن طريق الإجراءات الأولية أو الاستدلالية التي يقوم جهاز الضبطية القضائية وعن طريق الدعوى العمومية التي تحركها وتباشرها النيابة العامة".[3]

- **أهمية المكافحة الإجرائية:** إذا كانت الجريمة المعلوماتية مثلها مثل غيرها من الجرائم من ناحية أركان الجريمة وعناصرها[4]، وتسير الدعوى الجنائية بالنسبة لها بذات المراحل التي تسير فيها الدعوى الجنائية في الجرائم التقليدية، فإن الإجراءات المتبعة في سير هذه الدعوى سوف تختلف عن تلك المتبعة في الجرائم التقليدية كنتيجة منطقية لاختلاف الجريمة المعلوماتية عن الجرائم التقليدية لكونها جريمة من نوع خاص، ولذلك وجدت معظم التشريعات العقابية نفسها إزاء مشكلة أخرى لمكافحة الجريمة المعلوماتية.[5]

---

[1] أوهايبة عبد الله، (2008)، شرح قانون الإجراءات الجزائية الجزائري-التحري والتحقيق-، دار هومة للطباعة والنشر والتوزيع، 2008، ص22.

[2] طرشي نورة، مرجع سابق، ص90.

[3] أوهايبة عبد الله، مرجع سابق، ص22.

[4] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان، 2011، ص76.

[5] طرشي نوة، مرجع سابق، ص88.

ذلك أنه حتى وإن المكافحة من الناحية العقابية الموضوعية قامت بسن تشريعات جديدة أو تعديل التشريعات القائمة احتراما لمبدأ الشرعية الذي مفاده "لا جريمة ولا عقوبة إلا بنص"، فإن القصور التشريعي الإجرائي كان حجر عثرة ثانية في خطوات المكافحة التي بذلتها الدول منذ ظهور الجريمة المعلوماتية وذلك للأسباب التالية:[1]

- **البيئة الرقمية للجريمة المعلوماتية:** وجود الجريمة المعلوماتية في بيئة لا تعتمد التعاملات فيها على الوثائق والمستندات المكتوبة، بل تعتمد على نبضات الكترونية غير مرئية لا يمكن قراءتها إلا بواسطة الحاسبات الآلية.
- **آثار الجريمة المعلوماتية:** البيانات التي يمكن استخدامها كأدلة ضد الفاعل، يمكن في وقت قصير جدا العبث بها أو محوها بالكامل وبالتالي لا أثر للجريمة بعد ارتكابها.
- **هوية المجرم المعلوماتي:** آثار الجرائم المعلوماتية تعتمد على الخداع في ارتكابها، والتضليل في التعرف على مرتكبيها،فالمعتدون أو الجانحون في المجال المعلوماتي لهم القدرات الفائقة على إخفاء هويتهم عند ارتكابهم جرائمهم كونهم في غالب الأحيان ذوي دراية ومعرفة عالية بتقنيات المعلوماتية المتطورة.

ثالثا/ التعاون الدولي في مواجهة الجريمة المعلوماتية: إن جرائم الحاسوب والانترنت جرائم عابرة للحدود، وقد يساهم أكثر من شخص في دول مختلفة في ارتكاب جريمة واحدة يقع ضحيتها عدد من الأفراد يقيمون في بلدان متعددة، فتظهر مشكلة التعارض والاختلاف بين التشريعات الإجرائية في دول العالم.

فالتعاون الدولي هو من أهم سبل مكافحة جرائم الانترنت وملاحقة مرتكبيها فبغير التعاون الدولي يزداد معدل ارتكاب الجرائم ويطمئن مرتكبوها من عدم إمكانية ملاحقتهم إذ يكون من السهل عليهم التنقل من دولة إلى أخرى تبيح القوانين السارية ما ارتكبوه من جرائم.[2]

أ.التعاون القضائي: إن إجراءات التحقيق والملاحقة القضائية في جرائم الانترنت تقتضي تتبع النشاط الإجرامي الأمر الذي يستوجب تقصي آثار الجريمة من مصدرها إلى غاية

[1] إسحاق إبراهيم منصور، المبادئ الأساسية في قانون الإجراءات الجزائية، ديوان المطبوعات الجامعية، الجزائر، 1979، ص09.

[2] علي حسين الطوابلة ، التعاون القضائي الدولي في مكافحة الجريمة الالكترونية، جامعة العلوم التطبيقية، الأردن، ص1.

تنفيذها وتحديد مواقع الأضرار التي مستها[1]، وذلك من خلال مجموعة متنوعة من مقدمي خدمات الانترنت أو الشركات المقدمة لتلك الخدمات مع توصيل أجهزة الحاسب الآلي بالانترنت، وحتى ينجح المحققون في ذلك فعليهم أن يتتبعوا أثر قناة الاتصالات بأجهزة الحاسب الآلي المصدرية والجهاز الخاص بالضحية أو بأجهزة أخرى تعمل مع مقدمي خدمات وسطاء في بلدان مختلفة[2]، ولتحديد مصدر الجريمة غالبا ما يتعين على أجهزة إنفاذ القانون الاعتماد على السجلات التاريخية التي تبين متى أجريت تلك التوصيلات ومن أين ومن الذي أجراها، وفي أحيان أخرى قد يتطلب إنفاذ القانون تتبع أثر التوصيل ووقت إجرائه، وعندما يكون مقدمو الخدمات خارج نطاق الولاية القضائية للمحقق وهو ما يحدث غالبا فإن أجهزة إنفاذ القانون تكون بحاجة إلى مساعدة من نظرائها في ولايات قضائية أخرى، بمعنى الحاجة إلى ما يسمى بالتعاون القضائي،[3]ومن أهم صور التعاون القضائي هما التعاون الأمني والمساعدة القضائية الدولية.

- **التعاون الأمني الدولي:** حتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول فإنها تحتاج إلى قدر من النظام والأمن، وتشكل الجريمة إحدى القضايا الرئيسية في الكثير من دول العالم، وتشغل بال الحكومات والمختصين والأفراد على حد سواء، ولقد أثبت الواقع العملي أن أي دولة لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل في كافة ميادين الحياة[4]، فنتيجة للتطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات وظهور الانترنت والانتشار الواسع والسريع لها أدى إلى ظهور أشكال وأنماط جديدة من الجرائم منها الجرائم المتعلقة بشبكة الانترنت وهي نوع من الجرائم المعلوماتية[5]، التي باتت تشكل خطرا لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب، بل تعدت

---

[1]قرزان مصطفى، الآليات الدولية لمكافحة الجريمة الالكترونية، مداخلة مقدمة في الملتقى الدولي حول التنظيم القانوني للانترنت والجريمة الالكترونية، جامعة زيان عاشور، الجلفة، 2009، ص6.

[2]يوسف حسن يوسف ، الجرائم الدولية للانترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، 2011، ص143.

[3]الغافري حسين بن سعيد، الجهود الدولية في مواجهة جرائم الانترنت، ورقة عمل مقدمة للأمانة العامة لمجلس التعاون الخليجي خلال اجتماع اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم الالكترونية الأول، الرياض، 2004، ص3.

[4]يوسف حسن يوسف، مرجع سابق، ص6.

[5]الغافري حسين بن سعيد، مرجع سابق، ص3.

إلى أمن البنى الأساسية الحرجة ومع تميزها بالعالمية فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرامي الجنائي، بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالانترنت وتعميمها[1]، ويشن الهجوم الفيروسي من حواسيب موجودة في دولة أخرى، وتقع الآثار المدمرة لهذا الهجوم في دولة ثالثة، لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة ونتعاون من خلال أجهزة الشرطة في الدول المختلفة خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الفارين من وجه العدالة.[2]

- **جهود المنظمة الدولية للشرطة الجنائية للأنتربول:** إن البدايات الأولية للتعاون الدولي الشرطي يرجع إلى عام 1904 عندما تم إبرام الاتفاقية الدولية الخاصة بمكافحة الرقيق الأبيض بتاريخ 1904/05/18 والتي نصت في مادتها الأولى على: "تتعهد كل الحكومات المتعاقدة بإنشاء أو تعيين سلطة لجمع المعلومات الخاصة باستخدام النساء والفتيات لغرض الدعارة في الخارج، ولهذه السلطة الحق في تخاطب مباشرة الإدارة المماثلة لها في كل الدول الأطراف المتعاقدة"[3]، بعد ذلك أخذ التعاون الشرطي الدولي يأخذ صور المؤتمرات الدولية، أولها وأسبقها تاريخيا كان مؤتمر موناكو سنة 1914 والذي وضع رجال الشرطة والقضاء والقانون لـ 14 دولة وذلك لمناقشة ووضع أسس التعاون الدولي في بعض المسائل الشرطية خاصة ما يتعلق بمدى إمكانية إنشاء مكتب دولي للتسجيل الجنائي وتنسيق إجراءات تسليم المجرمين إلا أنه ونتيجة لقيام الحرب العالمية الأولى لم يحقق المؤتمر أي نتائج عملية[4]، إلا أنه بعد اندلاع الحرب العالمية الثانية توقفت اللجنة عن أعمالها، حتى وضعت الحرب أوزارها عام 1946، وانعقد مؤتمر بروكسل سنة 1946، وانتهى الاجتماع إلى إحياء اللجنة الدولية للشرطة الجنائية وغير اسمها ليصبح المنظمة الدولية للشرطة الجنائية، وتهدف المنظمة الدولية للشرطة الجنائية طبقا للمادة 2 من القانون الأساسي إلى:

[1] يوسف حسن يوسف، مرجع سابق، ص145.

[2] الغافري حسين بن سعيد، مرجع سابق، ص6.

[3] الغافري حسين بن سعيد، مرجع سابق، ص6.

[4] يوسف حسن يوسف، مرجع سابق، ص146.

- ✓ تأمين وتنمية التعاون المتبادل عل أوسع نطاق بين كافة سلطات الشرطة الجنائية في إطار القوانين القائمة في مختلف البلدان والإعلان العالمي لحقوق الإنسان.
- ✓ إنشاء وتنمية كافة المؤسسات القادرة على المساهمة الفعالة في الوقاية من جرائم القانون العام ومكافحتها.[1]

بالتالي تهدف هذه المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة.

- **القيام بعمليات أمنية مشتركة:** حيث يتم تعقب جريمة الانترنت وتتبع الأدلة الرقمية وضبطها والقيام بعمليات التفتيش العابر للحدود لمكونات أجهزة الإعلام الآلي والأنظمة المعلوماتية وشبكات الاتصال بحثا عن ما قد تتضمنه من أدلة وبراهين وهذه الإجراءات تستدعي كلها تعاونا وليا مكثفا لا سيما العمليات الفنية والأمنية كما من شأنها صقل مهارات وخبرات القائمين على مكافحة تلك الجرائم.[2]

أ.المساعدة القضائية: تعرف المساعدة القضائية دوليا بأنها: "كل إجراء قضائي تقوم به دولة منشأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم"[3]، وتتخذ المساعدة القضائية في المجال الجنائي عدة منها:

- **تبادل المعلومات:** ويتم بواسطة تبادل البيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية بصدد النظر في جريمة ما.
- **نقل الإجراءات:** يقصد به قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى ما توافرت شروط معينة من أهمها التجريم المزدوج، ويقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات، ولقد أقرت العديد من

---

[1] الحاج الطاهر زهير، آليات الوقاية من الجريمة المعلوماتية ومكافحتها، مذكرة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، 2013، ص185.

[2] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات (دراسة مقارنة)، دار الفكر الجامعي، الإسكندرية، 2007، ص 147.

[3] لغافري حسين بن سعيد، مرجع سابق، 8.

الاتفاقيات الدولية والإقليمية بهذه الصورة كإحدى صور المساعدة القضائية الدولية كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية.[1]

أ. **تسليم المجرمين:** استقر فقه القانون الدولي على اعتبار تسليم المجرمين شكلا من أشكال التعاون الدولي في مكافحة الجريمة والمجرمين وحماية المجتمعات من المخلين بأمنها واستقرارها، وهذا النوع من التعاون الدولي هو نتيجة طبيعية للتطورات التي حدثت في كافة المجالات ومنها مجال الاتصالات وتقنية المعلومات، حيث لم تعد الحدود القائمة بين الدول تشكل حاجزا أمام مرتكبي الجرائم كما أن نشاطهم الإجرامي لم يعد مقتصرا على إقليم معين بل امتد إلى أكثر من إقليم[2]، بحيث بات المجرم منهم يشرع في التحضير لارتكاب جريمته في بلد معين ويقبل على التنفيذ في بلد آخر ويرتكب الفرار إلى بلد ثالث للابتعاد عن أيدي أجهزة العدالة، الجريمة إذا أصبح لها طابع دولي والمجرم ذاته أصبح مجرما دوليا، وهذا بالفعل ما ينطبق على الجرائم المتعلقة بالانترنت.

وإذا أمعنا النظر في نظام تسليم المجرمين، لوجدناه يقوم على أساس أن الدولة التي يتواجد على إقليمها المتهم بارتكاب أحد الجرائم العابرة للحدود ومنها الجرائم المتعلقة بالانترنت عليها أن تقوم بمحاكمته بمعرفة دولة أخرى مختصة[3]، وهو إذا يحقق مصالح الدولتين الأطراف في عملية التسليم، فهو يحقق مصلحة الدولة الأولى في كونه يساعدها على تطهير إقليمها من فرد خارج عن القانون ومن شأن بقائه فيها يهدد أمنها واستقرارها.[4]

خاتمة:

عرف العالم خلال السنوات الأخيرة تقدما غير مسبوق في مجالات الإعلام والاتصال، التي أصبحت تعتمد أكثر فأكثر على الابتكارات الجديدة في مجال المعلوماتية (الانترنت، الرقمنة...)، فقد أصبح من الواضح اليوم أن هناك ارتباط وثيق بين النتائج التي تقدمها باستمرار صناعة تكنولوجيا المعلومات والاتصالات وطرق ارتكاب الجرائم المعلوماتية، التي لا زالت مخاطرها في ازدياد مطرد مع ما تقدمه لها هذه التكنولوجيا الحديثة.

[1] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير ، جامعة باتنة، 2013، ص90.

[2] شريف سيد كامل ، الجريمة المنظمة في القانون المقارن، الطبعة الأولى، دار النهضة العربية، القاهرة، 2001، ص262.

[3] سعيداني نعيم، مرجع سابق، ص92.

[4] الغافري حسين بن سعيد، مرجع سابق، ص9.

حيث بدأت هذه الجرائم تهدد الاقتصاد العالمي نتيجة الخسائر الكبيرة الناتجة عنها، مما دفع هذه الدول إلى مواكبة هذا التطور التكنولوجي بوضع النصوص الملائمة لمختلف استعمالات الإعلام الآلي، كما تم وضع قوانين خاصة لمواجهة الإجرام المعلوماتي، أما في مجال الجهود الدولية المبذولة لمجابهة ظاهرة الإجرام المعلوماتي يمكن القول بأن بعض الاتفاقيات الدولية لا تزال تتخذ كمرجع لصياغة النصوص المتعلقة بوضع الإطار القانوني لحماية النظام المعلوماتي بشكل عام ومنها اتفاقية تريبس، بالإضافة إلى اتفاقية برن، واللتان تظلان من أهم الأطر القانونية القائمة كآليات دولية لفرض الحماية القانونية المطلوبة، والتي ظلت تدفع في اتجاه خلق ضوابط أخرى إذ تجدر الإشارة إلى معاهدة جنيف الخاصة بقانون العلامات التجارية ولائحتها التنفيذية والتي أبرزتها إلى وجود المنظمة العالمية للملكية الفكرية (الويبو)، ولقد تم التوصل من خلال هذه الدراسة إلى جملة من النتائج نذكر منها:

- استحداث تشريعات نموذجية لمكافحة الجريمة المعلوماتية يمكن تطبيقها عالميا، وقابلة للاستخدام مع مراعاة التدابير التشريعية القائمة على الصعيدين الوطني والإقليمي.
- ضرورة تعزيز الجهود الدولية الرامية إلى مكافحة الجريمة المعلوماتية بغرض صوغ صك شامل متعدد الأطراف، يضع معالم نهج دولي في مجالات التجريم والصلاحيات الإجرائية والولاية القضائية والتعاون الدولي.
- ضرورة مجانسة التشريعات الخاصة بالفضاء المعلوماتي والاستخدام الآمن للانترنت.

الإجراءات الوقائية من الجريمة المعلوماتية في التشريع الجزائري

Preventive measures against information crime in Algerian legislation

د. حافظي سعاد
أستاذة محاضرة أ
كلية الحقوق والعلوم السياسية
جامعة أبوبكر بلقا يد تلمسان

مقدمة

لا تقتصر حرية المعلومات اليوم على الشخص الطبيعي،و إنما يستفيد منها الأشخاص الحكمية أو المعنوية و هي تشمل تلقي المعلومات و نقلها و التماسها و هي ترتبط ارتباطا عضويا بحرية الصحافة و وسائل الإعلام و يتعين على الدول اتخاذ التدابير الفعالة لمنع الرقابة على هذه الوسائل بشكل يتعارض مع حق الأفراد في حرية التعبير.

و المعلوم أن لكل فكر أدوات للتعبير لحرية الفكر[1] يعبر عنها بإحدى وسائل التعبير و كل شخص يتمتع بحرية التعبير عن أفكاره لحرية التعبير تشمل حرية النشر و هي حرية الصحافة و الاتصال و الحصول على المعلومات و هي حق من حقوق المواطنة لضمان الإعراب عن فكره بالقول أو الكتابة أو التصوير أو عن طريق الراديو التلفزيون و الانترنت ...

من الملاحظ انه قد حدث خلال القرن العشرين نمو نوعي لحجم و مقاييس المعلومات و المعارف المتداولة و يسمى ذلك بالانفجار المعلوماتي أو الثورة المعلوماتية و باتت صناعة المعلوماتية في العقود الأخيرة الموجه الرئيسي لتسريح التقدم العلمي و كان لظهور الانترنت أكثر كبير في انتقال المعلومات و تداولها و الاستفادة منها في وقت قياسي في أي مكان في العالم،فالانترنت ساهم بشكل لا نظير له في صناعة المعلومات و ثورتها فهو احد العناصر الرئيسية التي ترتكز عليها تكنولوجيا المعلومات.[2]

---

[1] SNOUSSI Mounir ,L'assemblé nationale constituante et les droits fondamentaux,collogue international Les droits fondamentaux dans la constitution regards croises !17-19 avril 2009 sous la direction de Mohamed Naceur LOUED,p.19..

[22] – نهلا عبد القادر مومني ،الجرائم المعلوماتية ،دار الثقافة لنشر و التوزيع ،2008 ص.34

Cf. Les publication Affaire handysidec.royaume uni saisie et confiscation en Angleterre d'un livre juge observe et condann²tion de l'éditeur a une amende , les

خضم هذه الثورة المعلوماتية ظهر مصطلح جديد للجريمة، وهو ما يعرف بجرائم المعلوماتية او الجريمة الالكترونية والتي تعد اخطر أنواع الجرائم في عصرنا الحالي لما لها من تأثير كبير على مكونات المجتمع، حيث يترتب على انتشارها إضرار بالغة في حق الأفراد والمؤسسات وحتى الدول ذاتها ومن هنا تبرز **أهمية دراسة موضوع** فنظومة الأمن القومي لأي دولة قد يتم اختراقها من إي نوع من المجرمين الالكترونيين كالهاكرز مثلا،فالآمر لا يحتاج أكثر من شخص اعتاد الإجرام الالكتروني لكي يقوم باختراق مواقع الجهات الأمنية والاطلاع على أسرارها وخصوصياتها. ومما هو جدير بالذكر إن الجرائم الالكترونية هي ظاهرة إجرامية جديدة ومستجدة تستدعي دق ناقوس الخطر فهي تستهدف الاعتداء على المعطيات بدلالاتها التقنية الواسعة وهي موجهة للنيل من الحق في المعلومات وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات الانترنت.

ويشير مصطلح الجريمة الالكترونية الى أي جريمة قد يستخدم الحاسوب في ارتكابها وقد يكون هو الهدف، ويمكن تعريفها على أنها:"أي مخالفة ترتكب ضد أفراد أو جماعات بدافع جرمي ونية الإساءة لسمعة الضحية أو لجسدها أو عقليتها سواء كان ذلك بطريقة مباشرة أو غير مباشرة وان يتم ذلك باستخدام وسائل الاتصال الحديثة مثل الانترنت(غرف الدردشة أو البريد الالكتروني أو المجموعات..الخ)".[1]

وسنحاول من خلال هذه الدراسة التطرق للإجراءات الوقاية المتخذة من خلال قانون الوقاية من جرائم تكنولوجيا المعلومات والاتصال ومن خلال قانون العقوبات . فماهي الإجراءات الوقائية المتخذة للوقاية من جرائم المعلوماتية في التشريع الجزائري ؟

---

interdictions de publier arrêt 7 décembre 1976recherche d'abord si les mesurées ayant porté atteinte a la liberté expression de M.HANDJSIDE qui se plaignant d'une différence arbitraire de traitement ;affaire Sanday tires c.royaume –uni n1 interdiction faite présidium de publier des information sur des procès civils en cours le requérants demanda vient ai titre de satisfaction équitable le remboursement de buns frais et dépens dans la procédure arret du 6 novembre 1980 la cour admet avec le gouvernement que le pleinement des frais en vertu de l'article 5 n'est pas automatique a mais relève son pourvoir d'appréciation،

[1]–د.حسين شفيق، الإعلام الجديد والجرائم الالكترونية –التسريبات–التجسس–الإرهاب الالكتروني، دار فكر وفن للطباعة والنشر والتوزيع، مدينة السادس من اكتوبر،2014–2015، ص16.؛ خضرخضر ، مدخل إلى الحريات العامة وحقوق الإنسان، المؤسسة الحديثة للكتاب، ط.3، 2008، ص.341؛–يحياوي نورة بن علي ،حماية حقوق الإنسان في القانون الدولي و الداخلي ،دار الهومة ط.2،2006 .

المطلب الأول: الإجراءات الوقائية من الجريمة المعلوماتية خلال قانون وقاية من جرائم تكنولوجيا إعلام واتصال

يهدف القانون 09-04 إلى حماية أنظمة المعالجة آلية للمعطيات وحمايتها من الجرائم كماله مجال في التحقيق فمع مراعاة لسرية الاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزماته التحريات أو التحقيقات مراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها والقيام بإجراء التفتيش أو الحجز داخل أنظمة المعلومات كما يمكن مراقبة الاتصالات الالكترونية في أعمال إرهابية لمقتضيات تمس أمن الدولة ومؤسساتها والدفاع الوطني وكذلك لمقتضيات التحقيق في قضية بحيث يصعب الوصول إلى نتيجة دون اللجوء إلى المراقبة الالكترونية يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية اذن لمدة 6 أشهر قابلة للتمديد ودلك على أساس تقرر يبين طبيعة الترتيبات التقنية المستعملة إضافة الى قواعد خاصة بعملية التفتيش وطلب مساعدة دولة أجنبية من أجل تفتيش منظومة معلوماتية موجودة بالخارج تطبيقا لمبدأ المعاملة بالمثل . وكداك حجز معطيات وبيانات ومنع الوصول الى المعطيات محتوى الجرم وحفظ المعطيات المتعلقة بحركة السير حسب المادة 10 من القانون 09-04 إضافة الى التزامات مقدم الخدمة بالتعاون مع السلطات القضائية ويعاقب الشخص الطبيعي من من 6 أشهر الى 5 سنوات وبغرامة من 50.000دج الى 500.000دج إضافة الى التزامات مقدمي خدمة الأنترنت بمنع الوصول الى بيانات المخالفة للنظام العام والتي تشكل جرما عن طريق سحب محتوياتها وضع ترتيبات تقنية بمنع الوصول إليها حسب المادة 12 من القانون 09-04 كما تنشئ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته حيث تتولى التنسيق وتنشيط عمليات الوقاية من جرائم الإعلام ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بالإعلام وهدا حسب المادة 14 من قانون 09-04 السالف الذكر ويكون الاختصاص للمحاكم الجزائرية ادا كانت الجرائم مرتكبة خارج الإقليم الجزائري عندما يكون مرتكبيها أجنبيا وتستهدف مؤسسات الدولة ويمكن طلب مساعدة قضائية دولية بشرط عدم المساس بسيادة مع إجراء التحفظ إما عن طريق الفاكس أو البريد الالكتروني .

المطلب الثاني: الإجراءات الوقائية من الجريمة المعلوماتية من خلال قانون عقوبات والقرار الوزاري المشترك

حيث نصت المادة 87 منه يعاقب بالسجن المؤقت من 5الى 10 سنوات وبغرامة من 100.000دج الى 500.000دج كل جزائري أو أجنبي مقيم بالجزائر بطريقة شرعية أو غير شرعية يسافر أو أية تحاول السفر الى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تدبيرها وأضافت الفقرة الأخيرة يستخدم تكنولوجيا الإعلام والاتصال لارتكاب الأفعال المذكورة .

ونصت المادة 87 مكرر 12 يعاقب بالسجن المؤقت من 5سنوات الى 10عشر 10 سنوات وبغرامة من 100.000دج الى 500.000دج كل من يستخدم تكنولوجيا الإعلام والاتصال لتجنيد الأشخاص لصالح إرهابي أو جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام هدا القسم أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها أو ينشر أفكارها .

و تنص المادة 394 مكرر 8 دون الإخلال بالعقوبات الإدارية المنصوص عليها يعاقب بالحبس من سنة الى ثلاث سنوات وبغرامة من من 2.000.000دج الى 10.000.000دج أو بإحدى هاتين العقوبتين فقط مقدم خدمة الأنترنت بمفهوم المادة 2 من القانون 09-04 المؤرخ في 5 غشت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها التي لا يقوم رغم اعداره من الهيئة الوطنية المنصوص عليها في القانون المذكور أو صدور أو حكم قضائي يلزمه بدلك بالتدخل الفوري لسحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا ، بوضع ترتيبات تقنية تسمح بتخزين أو بسحب المحتويات المتعلقة بالجرائم المنصوص عليها في الفقرة ا أو جعل الدخول اليها غير ممكن.[1]

و قد صدر مؤخرا قرار وزاري مشترك مؤرخ في 17 ديسمبر 2017 يحدد التنظيم الداخلي لهياكل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتشمل مصالح الإدارة العامة وتشمل مكتب الموارد البشرية مكتب المالية والوسائل مكتب الوقاية والأمن وهناك مديرية المراقبة الوقائية واليقظة الالكترونية وتشمل مصلحة المراقبة

04- القانون 02/16 المؤرخ في14 رمضان 1437الموافق ل 19 يونيو 2016 قانون العقوبات يعدل ويتمم الأمر 66—156 المؤرخ في 18 صفر 1386 الموافق ل8 يونيو 1966 والمتضمن قانون العقوبات ج ر العدد37

الالكترونية مصلحة المتابعة والتحليل والتعاون ويلحق به مركز العمليات التقنية والملحقات ومصلحة المراقبة الالكترونية مكتب تنسيق النشاطات مكتب مراقبة الاتصالات ومكتب مراقبة شبكات الاتصالات السلكية واللاسلكية مكتب مراقبة شبكة الانترنت وهناك مصلحة المتابعة التحليل والتعاون مكتب جمع معلومات ومكتب الوقاية والمتابعة ومكتب الاتصال والتعاون ويشتمل مركز العمليات التقنية على مكتب أنظمة المراقبة الهاتفية ومكتب أنظمة مراقبة الانترنت ومكتب أنظمة التموقع الجغرافي ومراقبة الاتصالات ومكتب الدعم التقني وتشمل الملحقة الجهوية مكتب الإدارة العامة ومكتب المراقبة الالكترونية وتشمل مصلحة المتابعة التحليل والتعاون مكتب جمع ومركزة استغلال المعلومات ومكتب الوقاية والمتابعة ومكتب الاتصال والتعاون ويشتمل مركز العمليات التقنية مكتب أنظمة المراقبة الهاتفية مكتب مراقبة الانترنت مكتب أنظمة التموقع الجغرافي ومراقبة الاتصالات مكتب الدعم الفني وتشمل الملحقة الجهوية مكتب الإدارة والمراقبة والمتابعة والتحليل والعمليات التقنية وتشمل مديرية التنسيق مصلحة الدراسات والخبرات القضائية ومصلحة منظومة الإعلام ومصلحة الدراسات والخبرات مكتب التقنيات الرقمية وقاعدة المعطيات ومكتب الدراسات وتشمل مصلحة منظومة الإعلام مكتب الأبحاث مكتب ادارة شبكة الإعلام مكتب امن منظومة الإعلام [1]

وقد صدر مؤخرا المرسوم الرئاسي 19-172 المؤرخ في 3 شوال 1440 الموافق ل6 يونيو 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها فالهيئة مؤسسة عمومية ذات طابع إداري تمتع بالشخصية المعنوية والاستقلالية المالية توضع تحت سلطة وزارة الدفاع الوطني .

ويحدد مقر الهيئة بمدينة الجزائر تتشكل من مجلس التوجيه ويتشكل من ممثلي وزارات وزارة الدفاع الوطني الوزارة المكلفة بالداخلية وزارة العدل الوزارة المكلفة بالمواصلات السلكية واللاسلكية وتتكلف حول مسائل تطوير التعاون مع المؤسسات والقيام دوريا بتقييم حالة التهديد في مجال جرائم المتصلة بتكنولوجيا الإعلام والاتصال تقييم أي اقتراح كل نشاط يتصل بالبحث دراسة التقرير السنوي لنشاطات الهيئة إبداء الرأي في كل مسالة تتصل بمهام الهيئة المساهمة في ضبط المعايير القانونية في مجال اختصاصه إما المديرية العامة

[1]– القرار الوزاري المشترك 17 ديسمبر 2017 يحدد التنظيم الداخلي للهياكل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ج ر العدد14 لسنة 2018

فتسهر على حسن سير الهيئة وإعداد مشروع الميزانية وإعداد وتنفيذ برنامج عمل الهيئة وتنشيط وتنسيق ومتابعة ومراقبة أنشطة هياكل الهيئة تنشيط وتنسيق ومراقبة أنشطة هياكل الهيئة تبادل المعلومات مع مثيلاتها الأجنبية بغرض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي الجرائم المتصلة ، تحضير اجتماعات مجلس التوجيه وإعداد التقرير السنوي لنشاطات الهيئة وتضم المديرية مديرية تقني مديرية الإدارة والمصالح وتقنية تقوم بمساعدة شرطة قضائية ووضع وسائل والأجهزة للمراقبة في مجال جرائم الإرهابية والتخريبية [1]

خاتمة

في الأخير نقول أن حرية المعلوماتية[2] تعد القاعدة الأساسية للحريات الأخرى ،و حرية المعلوماتية و منها حرية التعبير على الانترنت إلا أن إطلاقها وممارستها بحرية زائدة يؤدي ببعض مستعمليها الى تجاوز الحدود المشروعة واستخدامها لأغراض إجرامية تمس بكل مقومات المجتمع الوطني وحتى الدولي .

من بين النتائج المستخلصة انه:

- رغم تدارك المشرع الجزائري الفراغ القانوني في مجال الإجرام المعلوماتي وذلك بتجريم الاعتداءات الواردة على منتجات الإعلام الآلي إلا انه لم يستحدث نصا خاصا بالتزوير المعلوماتي.

- رغم تفطن المشرع الجزائري لهذا النوع من الجرائم بواسطة إحداثه لتعديلات في قانون العقوبات الجزائري وقانون 04/09 إلا أن ذلك لا يعتبر كافيا مع حداثة هذا النوع المستحدث من الجرائم الذي هو في تزايد مستمر.

و ما يمكن الخروج به كتوصيات هو كالتالي :

- يجب على المشرع أن يقوم بتطوير بيئته التشريعية تماشيا مع التطور السريع والملحوظ لهذه الجريمة .

- أنشاء أقسام متخصصة بالجرائم الالكترونية. إبرام اتفاقيات ومعاهدات للتعاون بين الدول لمكافحة الجريمة الالكترونية.

- ضرورة تخصيص شرطة جنائية خاصة وخبراء من ذوي الكفاءات العالية في مجال الانترنت.

---

[1]– المادة من 2 الى15المرسوم الرئاسي 19–172 المؤرخ في 3 شوال 1440 الموافق ل6 يونيو 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها ج ر ، العدد .37.

[2]cf,p, WACHSMAN, la liberté d'expression, liberte et droits fondamentaux sans la direction de R.cabrillac,M,Af ,ROCHE,TH ,REVET,9ed.,édit ,dalloz,2003pp.339 et s.

- على السلطات المختصة الإكثار من الحملات التوعية للمواطنين من اجل وضعهم في الصورة لتوخي الحيطة والحذر من هذه الجرائم التي تتزايد أكثر فأكثر.

- ضرورة تدريب وتأهيل أفراد الضبطية القضائية وكذا النيابة العامة على كيفية التعامل مع هذا النوع من الجرائم وتحقيق التعاون مع التقنيين من أصحاب الخبرة. ووضع إجراءات كالتحقيق والمحاكمة للجريمة الالكترونية تختلف عن الجريمة التقليدية.

- تدريس مواد الأنظمة المعلوماتية والجرائم التي قد تنشا منها يشكل بسيط في كليات الحقوق والمعاهد القضائية.

مدى فعالية الآليات القانونية لمواجهة متطلبات وخصوصية الجريمة المعلوماتية في ظل العولمة
(بين النص القانوني و تطور الجريمة)

The effectiveness of legal mechanisms to address the requirements and privacy of information crime in light of globalization
(between the legal text and the development of crime)

د. برنـــي كريمة أستاذ محاضر قسم (أ)
كلية الحقوق
جامعة الإخوة منتوري قسنطينة – الجزائر

مقدمة :

بالرغم من المزايا والفوائد الجمّة التي تحققت يوما بعد يوم في كل مجالات الحياة بفضل تقنيات وسائل التكنولوجيا المعلومات والاتصال ، إلا أن الاستخدام المتنامي لهذه التقنيات انعكس في الوقت نفسه، على بعض الجوانب السلبية التي تمثل تهديدا خطيرا للأمن والاستقرار في المجتمع ، جراء سوء استخدام هذه التقنية واستغلالها على نحو غير مشروع وبطرق من شأنها أن تلحق الضرر بمصالح الافراد والمؤسسات.

و مع تزايد نسبة الجرائم المعلوماتية وتنوع طرقها لا شك أنها تلحق خسائر مادية كبيرة وفادحة أكثر مما تسببه الجرائم التقليدية ليس فقط على مستوى الفرد بل تتعداه إلى مستوى المنظمات والجهات والمؤسسات وهذا بالطبع يؤثر بشكل سلبي على التنمية الاقتصادية وتشكل عبئا اقتصاديا ضخما من خلال توسيع الاجهزة الامنية والقضائية ، مما ينجم عنه إعاقة التنمية ، هذا أوجب تطوير البنية التشريعية الجزائية الوطنية بذكاء تشريعي مماثل تعكس فيه الدقة الواجبة علي المستوى القانوني وسائر جوانب وأبعاد تلك التقنيات الجديدة[1] ، بما يضمن في الأحوال كافة احترام مبدأ شرعية الجرائم والعقوبات من ناحية ، ومبدأ الشرعية الإجرائية من ناحية أخرى ، وتتكامل فيه في الدور والهدف مع المعاهدات الدولية .

[1]- ذياب موسى البداينة ،الجرائم الالكترونية : المفهوم والأسباب ، كلية العلوم الاستراتيجية عمان ، الاردن ،2014 ، ص 121.

استقر الفكر القانوني على ضرورة إيجاد نصوص خاصة لحماية المال المعلوماتي ، وقد استجابت عدة دول لهذه الحاجة بسنها قوانين تناولت في طياتها تعريف الجريمة المعلوماتية وأنواعها وخصائصها وأركانها والعقوبات المقررة[1] لها، ومنها التشريع الجزائري الذي تدارك مؤخرا الفراغ القانوني في مجال الجريمة المعلوماتية وذلك باستحداث نصوص تجريمية خاصة لقمع الاعتداءات الواردة على المعلوماتية بموجب تعديل قانون العقوبات رقم **04/15** المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات[2]، باستحداث القسم السابع مكرر ضمن الفصل الثالث من الباب الثاني من الكتاب الثالث تحت عنوان **المساس بأنظمة المعالجة الآلية للمعطيات من المادة 394 مكرر إلى 394 مكرر** 7 من قانون العقوبات ، وكذا القانون رقم **09/04** المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته ، أما على المستوى الدولي فنجد أول اتفاقية حول الإجرام المعلوماتي كان بتاريخ 11/20/ 2001 التي تضمن مختلف أشكال الاجرام المعلوماتي أما المشرع الفرنسي فقد تناولها في المواد 323،1 إلى 326،6 من القانون العقوبات الفرنسي[3] .

نجد أن المشرع الجزائري اتخذ هذه الاجراءات اللازمة من أجل مقاومة الجريمة المعلوماتية المنصوص عليها في الاتفاقية الأورومتوسطية المؤرخة في 04/22 /2002 التي كانت تهدف إلى ربط الجهود بين الوحدة الاوربية والدول الاعضاء فيها ومابين الحكومة الجزائرية من جهة أخرى وقد صادفت الجزائر مع الدول الفرنسية في مجال مكافحة الإجرام[4] المنظم وذلك بتاريخ 2003/10/25 ودخلت حيز التنفيذ بموجب المرسوم الرئاسي رقم 37/56.

---

[1]- محمد علي العريان، الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر ، الاسكندرية ، 2004،ص 43

[2]_ القانون رقم 04/15 المؤرخ في 27 رمضان عام 1425 الموافق ل 10 نوفمبر سمة 2004 المعدل والمتمم للأمر رقم 156/66 المتضمن قانون العقوبات الجزائري المؤرخ في 08 جوان 1966 ، ج.ر،ع 71.

[3]الأمر رقم 66-156 المؤرخ في 8 جولية 1966 المتضمن قانون العقوبات ، ج،ر،ع 49 / القانون رقم 09/04 المؤرخ في 05 أ،ت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها ، ج،ر،ع 47 الموافق 16اوت 2009-

[4]- الاتفاقية الدولية حول الاجرام المعلوماتي أبرمت بتاريخ 2001/11/20 من طرف المجلس الاوروبي وتم وضعها للتوقيع منذ تاريخ 2001/11/22)-ذياب موسى البداينة، المرجع السابق ص 202

تجلى أهمية هذه الدراسة في إلقاء الضوء على الدور الذي يجب أن تضطلع به الدول والأفراد للتصدي لهذه الجريمة والوقاية منها، كما تستمد هذه الدراسة أهميتها ادراكا منا أن ظاهرة الجرائم المستحدثة ومنها الاجرام الالكتروني ومدى تأثيره على التنمية الاقتصادية - قد غدت تشكل تحدّيا حقيقيا للسياسات الجنائية السائدة وأجهزتها التشريعية والتنفيذية والقضائية.

وقد استفادنا كثيرا مما توصلت إليه الدراسات السابقة ذلك من خلال إطلاعنا على بعض المؤلفات والتي كان في مجملها قليلة من ناحية الإجرائية بالمقارنة بالرصيد العلمي القانوني في هذا المجال ، راجع لحداثة موضوع الاجرام المعلوماتي من ناحية -**الاطار التشريعي والتنظيمي**- الخاص به ، فقد تم الإلمام وجمع أكبر عدد ممكن من المراجع عبر شبكة الانترنت لإعداد هذه الدراسة النظرية للموضوع في غياب المراجع الحديثة باللغة العربية في المكتبات الوطنية.

من هذا المنطلق ، فإن الإشكالية التي أود إثارتها في هذا الورقة البحثية ، والنقطة التي تحتاج إلى تمحيص وتحليل عن مدى نجاعة السياسة التشريعية الجنائية الوطنية و الدولية للتصدي للجرائم المعلوماتية ؟ .

ــ إلى أي مدى ينعكس الاجرام المعلوماتي آثاره على التنمية الاقتصادية ؟.

-ما مدى ملائمة النص الجنائي للسلوك الاجرامي المعلوماتي المستحدث وفق التشريع الجزائري ؟.

وللإجابة على الإشكالات المطروحة أعلاه ، سنحاول تسليط الضوء على الشكل المستحدث للجريمة المعلوماتية مع إبراز أهم العوامل والاستراتيجيات المتبعة من أجل التصدي لهذه الظاهرة، لذا ارتأينا تقسيم موضوع المداخلة إلى مبحثين أساسيين ، حيث سيتم دراسة في **المبحث الأول** الإطار المفاهيمي للجريمة المعلوماتية وإبراز مختلف الصور أو الآليات التي تنفد بها هذه الجرائم من خلالها ، في حين أخصص **المبحث الثاني** دراسة مدى خصوصية المتابعة بالجريمة المعلوماتية من خلال إجراءات التحري والتحقيق و وسبل تطويرها ،ثم **خاتمة** التي ستستوفي جملة من النتائج والتوصيات التي تخرج بها هذه دراسة.

المبحث الأول: الإطار المفاهيمي لجريمة المعلوماتية

لا جدال في اعتبار الجرائم المعلوماتية من أخطر وأعقد الجرائم وتأتي في مقدمة الأشكال الجديدة للجريمة المنظمة وخطورة هذه الجرائم نابعة من طبيعتها المتميزة والمعقدة من حيث ذاتية أركانها وحداثة أساليب ارتكابها والبيئة التي ترد عليها وخصوصية مرتكبيها ووسائل كشفها، فهي

جريمة تقنية سهلة الارتكاب ، تنشأ في الخفاء وفي بيئة الكترونية افتراضية[1]، إذ أن الجريمة المعلوماتية بوصفها ظاهرة إجرامية ذات طبيعة خاصة ، صعبت من جهود الفقه رجال القانون الجنائي للتوصل إلى اتفاق حول مصطلح دقيق وموحد يعبر عن هذه الظاهرة ، لذا يجدر بنا من خلال هذا المبحث أن نبين مفهوم الجريمة بشكل عام ، من خلال تجريم الفعل سن قانون خاص بالجرائم الالكترونية ، بشكل خاص مع تعريفات مقارنة لها في (المطلب الاول) ، ثم دراسة خصائص الجريمة المعلوماتية ضمن (المطلب الثاني).

المطلب الاول: مفهوم للجريمة المعلوماتية

إن مسألة تعريف للجريمة الإلكترونية كانت محلا لاجتهادات الفقهاء ، لذا ذهب بعض الفقهاء في تعريف الجريمة المعلوماتية مذاهب شتى ووضعوا تعريفات مختلفة ويتراوح تعريف الجريمة الالكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية ، وتعرف على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الهاتف ، لذا سنحاول التطرق للمفهوم اللغوي للجريمة المعلوماتية في " الفرع الأول " ثم نعرج لتبيان المفهوم الاصطلاحي لها ضمن " الفرع الثاني ".

الفرع الأول : التعريف اللغوي للجريمة المعلوماتية

هناك من عرفها على أنها الجرائم ذات الطابع المادي التي تمثل في كل سلوك غير قانوني من خلال استخدام الاجهزة الالكترونية ينتج منها حصول المجرم على فوائد مادية أو معنوية .

يقول فان دير هلستن ونيف" هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة ، وفي أغلب الاحيان تستخدم الافتراضية والحاسوب الالكترونية والرقمية وكلها تعكس فجوات مهمة في التعريف، وتعريف الجرائم الالكترونية على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال" ، وتتكون الجريمة الالكترونية أو الافتراضية [2] من قسمين هما " الجريمة crime و " الالكترونية cyber ويستخدم مصطلح الالكترونية لوصف فكرة جزء من الحاسوب أو عصر المعلومات .

---

[1]- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت ، دار الثقافة للنشر والتوزيع، الأردن ، بدون طبعة، 2011،ص 69.

[2]- الأمر رقم 66-156 المؤرخ في 8 جولية 1966 المتضمن قانون العقوبات، ج،ر،ع 49 / القانون رقم 09/04 المؤرخ في 05 أءت 2009 الموافق 16 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها ، ج،ر،ع 47.

أما الجريمة فهي السلوكيات والأفعال الخارجة عن القانون . والجرائم الالكترونية " هي المخالفات التي ترتكب ضد الافراد أو المجموعات من الافراد أو المؤسسات بدافع الجريمة ويقصد إيذاء سمعة الضحية أو أذى مادي أو معنوي للضحية مباشرة أو غير مباشرة باستخدام شبكات الاتصالات مثل الانترنت .

تعرف أيضا " على لأنها جريمة ذات طابع مادي ، تتمثل في كل فعل أو سلوك غير مشروع من خلال استعمال الوسائط الالكترونية مثل الحاسوب ، أجهزة النقال ، شبكات نقل المعلومات ، شبكة الانترنت ، حيث تتسبب في تحميل أو إمكانية تحميل المجني عليه خسارة[9]، وحصول أو إمكانية حصول مرتكبه على أي مكسب تهدف هذه الجرائم إلى الوصول غير المشروع لبيانات سرية غير مسموح بالإطلاع عليها ونقلها ونسخها أو حذفها ، أو تهديد وابتزاز الاشخاص والجهات المعنية بتلك المعلومات أو تدمير بيانات وحواسيب الغير بواسطة فيروسات".

أما ما جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين في فينا سنة 2000 تعريف الجريمة الالكترونية بأنها " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية ، أو داخل نظام حاسوبي ، والجريمة تلك تشمل من الناحية المبدئية ، جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية .

الفرع الثاني : التعريف الاصطلاحي للجريمة المعلوماتية

ثمة اختلاف بشان المصطلحات المستخدم للدلالة على الظاهرة الإجرامية الناشئة في بيئة الكمبيوتر والانترنت ، وهو اختلاف رافق مسيرة ونشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات والاتصالات ، فابتداء من مصطلح استخدام الكمبيوتر مرورا بمصطلح الاحتيال بواسطة الكمبيوتر، والجريمة المرتبطة بالكمبيوتر وجرائم التقنية العالية[1]، إلى جرائم الهاكرز أو الاختراقات لجرائم الانترنت وأخيرا السبير كرايم .

أما المشرع الجزائري فقد اصطلح على تسمية الجرائم الالكترونية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال وعرفها بموجب المادة 02 من قانون 04/09 على أنها " جرائم المساس بأنظمة المعالجة الآلية للمعطيات الآلية المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية [12]

[1]- حمود ابراهيم غازي، الحماية الجنائية للخصوصية والتجارة الالكترونية ، مكتبة الوفاء القانونية ، الاسكندرية، ط 01 ، 2014، ص 119

وقد عرفها الفقيه David Thomson أنها ذلك النشاط غير مشروع موجه انسخ أو تغير أو حذف أو الوصول إلى معلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه " ، أو هي أي نمط من أنماط الجرائم المعروفة في قانون عقوبات طالما كان مرتبطا بتقنية المعلومات "، وقد جاءت في توصية الامم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد بفينا سنة 2000 " هي الجريمة الناجمة عن إدخال بيانات عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدا من ناحية التقنية مثل تعديل الكمبيوتر".

كما عرفت الدكتورة هدى حامد قشقوش الجريمة المعلوماتية بأنها " كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب" ، وكذلك تعرف بأنها " الجريمة التي تلعب فيها البيانات الكمبيوتر والبرامج المعلوماتية دورا أساسيا ". وأنها " كل فعل أو امتناع من شأنه الاعتداء على الأمواج المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية ". ويعتبر هذا التعريف الاخير الرأي الراجح [13] لتبنيه من قبل العديد من الباحثين نظرا لشموليته على الطابع التقني المميز التي تنطوي عليه أبرز صور الجريمة الالكترونية

المطلب الثاني : خصائص الجريمة المعلوماتية

تميز الجريمة الالكترونية بخصائص و صفات تميزها عن غيرها من الجرائم الأخرى و من بين أهم هذه الخصائص ما يلي : مرتكب الجريمة الإلكترونية في الغالب شخص يتميز بالذكاء و الدهاء ذو مهارات عالية و دراية بالأسلوب المستخدم في مجال أنظمة الحاسوب الآلي و كيفية تشغيله وكيفية تخزين المعلومات و الحصول عليها، في حين أن مرتكب الجريمة التقليدية في الغالب شخص أمي بسيط متوسط التعليم .

مرتكب الجريمة الإلكتروني في الغالب يكون متكيفا اجتماعيا و قادرا ماديا، باعثه من ارتكاب جريمته الرغبة في قهر النظام أكثر من الرغبة في الحصول على الربح أو النفع المادي، في حين أن مرتكب الجريمة التقليدية غالبا ما يكون غير متكيف اجتماعيا و باعثه من ارتكاب الجريمة هو النفع المادي السريع .

تقع الجريمة الإلكترونية في مجال المعالجة الآلية للمعلومات و تستهدف المعنويات لا المادية .

الجريمة الإلكترونية ذات بعد دولي، أي أنها عابرة للحدود ، فهي قد تجاوز الحدود الجغرافية باعتبار أن تنفيذها يتم عبر الشبكة المعلوماتية وهو ما يثير في كثير من الأحيان تحديات قانونية إدارية فنية [14]، بل و سياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراء المتابعة الجنائية .

هي جريمة ناعمة ومغرية للمجرمين ، تنفذ بسرعة فهي صعبة الإثبات : ناعمة أي أنها لا تتطلب لارتكابها العنف ولا استعمال الأدوات الخطيرة كالأسلحة و غيرها ، فتقل بيانات ممنوعة أو التلاعب بأرصدة البنوك مثلا لا تحتاج إلا إلى لمسات أزرار ، تنفذ بسرعة أي أنها تميز بإمكانية تنفيذها بسرعة فأغلب الجرائم المعلوماتية ترتكب في وقت قصير جدا قد لا يتجاوز الثانية الواحدة ، وفي المقابل فهي صعبة الإثبات لعدم وجود الآثار المادية التقليدية (مثل بقع الدم ، التكسير ، خلع ...الخ) وهذا ما جعل وسائل الإثبات التقليدية غير كافية[1] ، مما أدى إلى البحث عن أدلة فعالة لإثباتها ، كاستخراج البصمات أو استعمال شبكية العين و مضاهاتها باستخدام وسائل آلية سريعة.

المبحث الثاني : إجراءات البحث و التحقيق الحديثة في الجرائم المعلوماتية

إن خصوصية الجريمة المعلوماتية ، أبرزت مشكلة مكافحة الاجرائية المعلوماتية خاصة من ناحية كيفية جمع الادلة الالكترونية ومدى حجتها ، وحتى تتوفر في الدليل الالكتروني المشروعية التي تشترطها القوانين في كافة التشريعات[2].

ومع إدراك الصعوبة التي تطرحها المواجهة الاجرائية لأشكال الاجرام الجديد التي أفرزتها مناخ المعالجة الآلية للمعطيات والتنبه لأثارها السلبية، بدأت مهمة معالجتها تحضى باهتمام متزايد من الحكومات وحتى العديد من الهيئات الدولية، فأخذ المختصون وخبراء الحسابات يركزون جهودهم البحثة وتجارهم العليمة على سدّ ثغرات الانظمة الامنية وتحسين وتطوير أساليب الحماية التقنية للنظم والبرامج المعلوماتية تجنبا لوقوع اعتداءات عليها أو بواسطتها .

وأمام هذا الوضع أثير التساؤل حول مدى صلاحية تطبيق إجراءات التحقيق التقليدية على الجرائم إلكترونية التي ارتكبت في عالم افتراضي غير ملموس،وهل هذا الوضع يجعل قانون الاجراءات الجزائية قاصرا عن الوفاء بمتطلبات الشرعية الجزائية في مواجهة هذا النمط الاجرامي الجديد ؟ وهل يقتضي على المشرع التدخل لتعديل واستحداث قواعد إجرائية خاصة تماشى والطبيعة المميزة للجرائم المعلوماتية ؟ ، لذا سنتطرق لدراسة إجراءات البحث والتحقيق التقليدية

1

[2]- عكور سمية ، الجرائم المعلوماتية وطرق مواجهتها ، قراءة في المشهد القانوني والأمني ، ورقة عمل مقدمة ضمن فعاليات الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، الأردن ، 2014، ص13.

في (المطلب الاول) ، ثم دراسة الاجراءات المستحدثة للتحقيق في الجريمة المعلوماتية ضمن (المطلب الثاني) .

المطلب الأول : قصور إجراءات البحث والتحقيق التقليدية في الجريمة المعلوماتية

لقد توسع تأثير التقنية المعلوماتية إلى الجانب الاجرائي من القانون الجزائي بشكل أوسع ، ولأن الجرائم التقليدية ترتكب في عالم ملموس يؤدي فيه السلوك المادي الدور الأهم على عكس الجريمة المعلوماتية التي ترتكب في مسرح إلكتروني افتراضي وغير مادي يختلف تماما عن المسرح التقليدي للجرائم المرتكبة فيه ، الأمر الذي دفع بالعديد من التشريعات إلى إعادة البحث عن صيغ جديدة لنصوص العقابية بما يتماشى مع هذا الاجرام المستحدث ذو التقنية العالية ،والعمل على تطوير وسائل الاثبات بما يتوافق والحقائق العلمية لتفادي هذا القصور.

غير أن المشرع الجزائري حينما أراد توسيع نطاق تطبيق إجراءات التحقيق التقليدية لتطال الجرائم الالكترونية، فهذه الاجراءات قد تثير إشكالات عملية تعود إلى خصوصية هذه الجرائم ، سنتطرق إلى دراسة التفتيش والمعاينة والخبرة في الفرعين الآتيين والتي هي في حاجة الى تحيينها لكي تتناسب مع طبيعة الاجرام المعلوماتي والدليل الذي يصلح لإثباتها .

الفرع الأول المعاينة التقنية

تعرف المعاينة على أنها " إجراء بمقتضاه ينتقل المحقق إلى مسرح الجريمة ليشاهد ويفحص بنفسه مكانا أو شخصا له علاقة بالجريمة ، لإثبات حالته والتحفظ على كل ما قد يفيد من الآثار في كشف الحقيقة [1] "

وتظهر أهمية المعاينة في أنها تنقل لجهات التحقيق والمحاكمة صورة كاملة للجريمة بكل ما يحتوية هذا الموقع من تفصيلات ، وحتى تقرر المعاينة أثارها وتفي بأغراضها ، نجد أن بعض التشريعات قد جزاءات جنائية على كل من يقوم بإجراء أي تغيير في المكان الجريمة .وتتم المعاينة في الجرائم الالكترونية كأي جريمة أخرى عن طريق الانتقال إلى مكان وقوع الجريمة ، غير ان الانتقال هنا يختلف حسب الجريمة الالكترونية المرتكبة وإذا كانت الجريمة واقعة على الاجهزة الالكترونية كجرائم الاعتداء على الحاسب الآلي الاقراص الممغنطة ، فالانتقال في هذه الحالة يكون ماديا إلى مسرح الجريمة لمعاينة مكونات التي تعد أدلة مادية تدل على وقوع الجريمة ، أما إذا كانت الجريمة واقعة على المكونات غير المادية للأجهزة الالكترونية أو بواسطتها ، فيكون

[1] - سعيدات نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير، جامع باتنة ، 2013/2012 ، ص 132.

الانتقال للمعاينة الكترونيا ، ويمكن للمحقق إجراء المعاينة الافتراضية أو الإلكترونية بالدخول والانتقال إلى مسرح الجريمة عبر الانترنت انطلاقا من مكتبه بواسطة الحاسب الموضوع تحت تصرفه ، ويلتزم المحقق عادة قبل البدء في المعاينة الالكترونية بجملة من التدابير الفنية والتحفظية التي تساعده في القيام بمهامه على أحسن وجه :

-الاستعلام المسبق عن مكان وقوع الجريمة، ونوع وعدد مواقع الاجهزة الالكترونية وشبكاتها وسائر ملحقاتها المتوقع مداهمتها .

-توفير الوسائل والإمكانات اللازمة من أجهزة وبرامج وأقراص صلبة ولينة التي يمكن الاستعانة بها في الفحص ، التشغيل ، الضبط وحفظ المعلومات .

-إعداد فريق من المتخصصين وأهل الخبرة في مجال تكنولوجيا الاعلام الآلي للاستعانة بهم عند الحاجة،و يعتمد المحقق الجنائي لإجراء المعاينة الإلكترونية بحثا عن الأدلة الرقمية على فحص مجموعة مصادر الدليل في البيئة الالكترونية التي ارتكبت فيها الجريمة المعلوماتية والمتمثلة عادة في مكونات أجهزة الحاسب الخاص بالمجنى عليه أو الجاني وملحقاتها وكذا الأنظمة الاتصال بالانترنت

ويمكن الاستعانة بالذكاء الاصطناعي لحصر الحقائق والاحتمالات والأسباب والفرضيات ومن ثم استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها الحاسب الآلي وفق برامج صممت خصيصا لهذا الغرض، حيث اثبتث تقنيات الحاسب الآلي نجاحها في جمع الأدلة الجنائية .

الفرع الثاني : التفتيش المعلوماتي

لقد أجمع الفقه الجنائي ، على أن التفتيش كإجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محا يتمتع بحرمة، وذلك بغرض إثبات وقوعها ونسبتها إلى متهم وفقا للضمانات والضوابط المقررة قانونا[1].

كما اتفقت معظم تشريعات الدول على أنه لا يجوز لهيئات التحقيق مباشرة إجراءات التفتيش إلا بعد التأكد من الوقوع الفعلي لجريمة الكترونية نص عليها القانون صراحة قي قانون العقوبات رقم 15/04 ، ولابد أن تحمل هذه الجريمة بمنظور القانون وصف جناية أو جنحة[2] ، ويستثنى

1- فهد عبد الله العبيدي العازمي، الاجراءات الجنائية المعلوماتية، رسالة لنيل درجة الدكتوراه في القانون، كلية الحقوق، القاهرة، 2012، ص268.

2- أمين أعزان، الجريمة المعلوماتية في التشريع المغربي ، مجلة العلوم القانوينة ، العدد01 ، 2016

من ذلك المخالفات بسبب ضعف خطورتها التي لا تستحق انتهاك حرمة الحياة الخاصة للأشخاص وسرية اتصالاتهم وحرمة منازلهم ".

بناء على ما سبق ، يتضح من نص المادة 66 من ق،إ،ج ،ج أن التفتيش ما هو إلا وسيلة للإثبات المادي هدفه هو ضبط الأدلة المادية الخاصة بالجريمة، مما يجعله يتنافى مع طبيعة غير المادية لبرامج وبيانات الحاسب الآلي، ومعطيات شبكة الانترنت.

وقد إتجه المشرع الجزائري نفس الاتجاه التي تحدث في عالم التكنولوجيات الحديثة، فقام بدوره استحداث نصوص قانونية جديدة أجاز فيها تفتيش المكونات المنطقية والمعطيات المعلوماتية للحاسب ، من بينها المواد 05 و04 من القانون رقم 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تسمح للسلطات القضائية المختصة في إطار قانون الاجراءات الجزائية ، وفي حالات نص المادة 04 من هذا القانون، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين المعلوماتية[20]إن إجراء التفتيش في الجريمة المعلوماتية تحتاج إلى تقنيات خاصة تختلف عن حالات التفتيش العادية التقليدية لان تفتيش نظم المعلومات ليس سهلة وتتطلب دراية ومعرفة بملفات أجهزة الاعلام الآلي وأماكن إخفاء المعلومات فيها لأنه يسهل اتلافها كليا أو جزئيا كما يصعب تحديد مكان الدليل[21].

المطلب الثاني : استحداث اجراءات البحث و تحقيق خاصة بالجرائم المعلوماتية

إذا كانت الثورة المعلوماتية قد أثرت على نوعية الجرائم التي صاحبتها بظهور أنمط مستحدثة من الجرائم عرفت بالجرائم المعلوماتية ، فإنها بالمقابل أثرت على وسائل إثبات هذه الجرائم ، إذ أصبحت الطرق التقليدية التي جاءت بها نصوص قانون الاجراءات الجزائية غير كافية لاستخلاص الدليل بخصوص هذا النوع الاجرامي المستجد الذي يحتاج إلى طرق وتقنية جديدة تتناسب مع طبيعته ,ويمكنها فك رموزه وترجمة ذبذباته إلى كلمات وبيانات محسوسة ومقروءة تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعلمية الخاصة.

و اعتبارا للطبيعة الخاصة للجرائم الالكترونية في عناصرها ووسائل وتقنيات ارتكابها اضطر المشرع الجزائي في العديد من الدول إلى إعادة النظر في كثير من المسائل الاجرائية الخاصة فيما تعلق بمسألة الاثبات ، باعتبارها أهم موضوعات هذا القانون ، لأن الدليل الذي يقوى على إثبات هذا النوع من الجرائم لابد أن يكون من ذات طبيعتها التقنية ، وهو الامر الذي لا تكون

فيه القواعد الإجرائية التقليدية التحقيق واستخلاص الدليل ، مما قد يؤدي في الغالب إلى إفلات العديد من المجرمين من العقاب.

وعلى ضوء ما تقدم ، كان لازم على المشرع التدخل بقواعد إجرائية جديدة أكثر فعالية تحمل معها طرقا إجرائية مدعمة من قبل التقنية ذاتها، يمكن للجهات المكلفة بالبحث والتحري عن الجريمة الالكترونية الاعتماد عليها في الكشف عن المجرم المعلوماتي والوصول إلى أدلة الاثبات بدقة وسرعة ، وهي الاجراءات التي سوف نقتصر على دراستها ضمن الفرعين الآتيين ، نتطرق في (الفرع الاول) للتسرب الإلكتروني ثم محاولة دراسة مراقبة الاتصالات الالكترونية و تجميعها ضمن (الفرع الثاني).

الفرع الأول : التسرب الالكتروني

إن التسرب من الاجراءات الشخصية ، والجريمة المعلوماتية من بين الجرائم التي تسمح فيها التشريعات اللجوء إلى مثل هذا الاجراء ، وقد كانت اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية سباقة إلى احتواء هذا الاجراء بنصها في المادة 20 على أساليب التحري الخاصة بما فيها التسري الذي عبرت عنه " الاعمال المستترة ". ولقد حددٌ المشرع الجزائري نطاق هذا الاجراء بالجرائم المذكورة على سبيل الحصر ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وقد نظمه المشرع في القسم الخامس من ق.إ ،ج وهو من ناحية الأمنية تلك العملية المحضر لها والمنظمة قصد التوغل داخل وسط لمعرفة أو استعلام عن نشاط جرمي وعرفة أدق التفاصيل فيه وخصوصياته إما من ناحية القانونية ، كما يجوز لضابط الشرطة المرخص له بإجراء عملية التسرب والأشخاص الذين يسخرون لهذا الغرض ، دون أن يكونوا مسؤولين جزائيا القيام بما يلي:

-اقتناء أو حيازة أو نقل او تسليم إو إعطاء مواد أو أموال أو منتجات أو وثائق أو كمعلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.

- استعمال او وضع تحت تصرف مرتكبي هذه الجرائم ، الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخريب أو الحفظ أو الاتصال .

ويحظر على المتسرب اظهر الهوية الحقيقية في أي مرحلة من مراحل الاجراءات مهما كانت الاسباب إلا لرؤسائهم ، لأن هذا سيؤدي إلى إفشال الخطة المتبعة في القبض على المشتبه فيهم وتعريض العضو المكشوف عن هويته للخطر، وهو ما أكده المشرع بموجب نص المادة 25 مكرر

12 " لا يجوز اظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا التسرب تحت هوية مستعارة في أي مرحلة من مراحل الاجراءات ".

كما عاقب المشرع كل من يكشف هوية ضابط أو أعوان الشرطة القضائية بالحبس من سنتين إلى خمس سنوات وبغرامة من 5000 دج إلى 200000 دج ، وإذا تسبب الكشف عن هوية في أعمال عنف أو ضرب أو جرح أحد هؤلاء الاشخاص أو أو أبناءهم أو أصولهم المباشرون، فتكون العقوبة الحبس من خمس سنوات إلى 10 سنوات والغرامة من 200000 إلى 500000 دج ،وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الاشخاص فتكون العقوبة الحبس من 10 إلى 20 سنة والغرامة من 500000 إلى 100000 دج[1].

ورغم أن المشرع أجاز مثل هذه الافعال التي تعتبر في حقيقة الأمر جرائم من أجل خلق الثقة وتعزيزها في ضباط الشرطة القضائية وأعوانهم المرخص لهم بإجراء عملية التسرب من قبل المشتبه فيهم والنجاح في إيهامهم بأنهم شركاء أو فاعلون مع ذلك منع المشرع هؤلاء الضباط أو الأعوان من أن يحرضوا المشتبه فيهم على ارتكاب الجريمة، بمعنى أنه يمنع على الضباط والأعوان المتسربين أن يخلقوا الفكرة الاجرامية للشخص الموضوع تحت المراقبة ودفعه لارتكاب الجريمة ، فهذا الفعل ممنوع تحت طائلة بطلان الاجراء .

الفرع الثاني : مراقبة الاتصالات الالكترونية و تجميعها

لقد أضفى المشرع الجزائري الحماية القانونية للبيانات ذات الطابع الشخصي من خلال المعالجة الآلية، بحيث اعترف المشرع الجزائري بها ضمن نص المادة 77 من الدستور **على أنه " يمارس كل واحد جميع حرياته، في إطار احترام الحقوق المعترف بها للغير في الدستور و لاسيما احترام الحق في الشرف ، وستر الحياة الخاصة "**، كما نصت المادة 46 من دستور سنة 1996 على أنه " لا يجوز انتهاك حرمة حياة المواطن الخاصة،وحرمة شرفه، ويحميها القانون ، سرية المراسلات والاتصالات الخاصة بكل أشكالها " ، إلا أنه في تعديل الدستور 2016 أضاف المشرع الجزائري تعديلات على المادة أعلاه ، تماشيا مع التطور الذي يشهده العالم في مجال حماية البيانات الشخصية على أنه " لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية ،

---

[1] أنظر المادة 65 مكرر 14 من الأمر رقم 155/66 المعدل والمتمم بموجب المادة 14 من قانون رقم 06/ 23 المتضمن قانون العقوبات الجزائري.

ويعاقب القانون انتهاك هذا الحكم "[1]، وقد تضمن قانون رقم 04/09 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها إجراءات مراقبة الاتصالات الالكترونية ، وتفتيش وحجز المنظومة المعلوماتية ، سنتطرق إلى إجراءات تفتيش المنظومة المعلوماتية أولا، ثم دراسة حجز المعطيات المعلوماتية ثانيا .

أولا : إجراءات تفتيش المنظومة المعلوماتية

نصت المادة 05 من القانون رقم 04/09 على أنه يجوز للسلطات القضائية المختصة ، و كذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية ، وفي الحالات المنصوص عليها في المادة 04 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى :

- منظومة معلوماتية أو جزء منها و كذلك المعطيات المعلوماتية المخزنة فيها.
- منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة – ا – من هذه المادة 04 ، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوثة عنها مخزنة في منظومة معلوماتية أخرى، و أن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى ، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك. وإذا تبين مسبقا بأن المعطيات المبحوث عنها ، و التي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا للمبدأ المعاملة بالمثل.

و المشرع الجزائري في المادة الخامسة من القانون رقم 04/09 نص على التفتيش المنصوص عليها في قانون الإجراءات الجزائية ، وحتى و أن اختلف مضمونه عن التفتيش العادي بحيث توفر شروط التفتيش المنصوص عليها في المادة 46 من القانون الإجراءات الجزائية مع مراعاة أحكام الفقرة الأخيرة منها لأننا بصدد جرائم معلوماتية.

ثانيا :حجز المعطيات المعلوماتية

أكدت المادة 06 من القانون رقم 04/09 ، أنه عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة ، يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة

[1] القانون رقم 16/01 المؤرخ في 06 مارس 2016 المتضمن التعديل الدستوري ، ج،ر،ع 14

لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز و الوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية .

غير أن القانون رقم 04/09 أجاز إجراء التفتيش على المنظومة المعلوماتية عن بعد ، وهذا إجراء جديد بحيث يمكن الدخول إليها دون إذن صاحبها بالدخول في الكيان المنطقي للحاسوب، للتفتيش عن أدلة في المعلومات على دعامة مادية أو نسخها للبحث عن الدليل فيها ،كما نص المشرع الجزائري ، و دائما في نفس القانون 04/09 على إجراء آخر يسهل عملية التفتيش في الفقرة الأخيرة من المادة 05 ، وهذا الإجراء يتمثل في اللجوء إلى الأشخاص المؤهلين كالخبراء والتقنيين المختصين في الإعلام الآلي وفن الحاسوبات لإجراء عمليات التفتيش على المنظومة المعلوماتية[1]، و جمع المعطيات المتحصل عليها و تزويد السلطات المكلفة بهذه المعلومات .

الخاتمة :

في ختام هذه الدراسة ، نخلص اننا اصبحنا نواجه واقعا ملحا على التدخل التشريعي لتنظيم التعاملات الالكترونية بصفة عامة ، قبل إصدار القوانين اللازمة لمواجهة الجرائم المعلوماتية ، إذ أصبحت اليوم تغطي معظم التعاملات اليومية في مختلفا الحالات ورغم ما وفرته من تسهيلات، إلا أنها في المقابل فتحت الباب على مصراعيها لتطور وسائل وأدوات لتنفيذ الجرائم المعلوماتية، وجعلها أكثر تعقيدا ، إن لم تتضافر الجهود جميع الاطراف الفاعلة في الساحة المعلوماتية ، وأمام هذا الوضع أصبح لازما على الدول الإسراع في اتخاذ الاجراءات اللازمة لتطوير آليات التصدي لمثل هذه الجرائم وتعزيز التصدي الدولي في هذا المجال.

و بما أن ظاهرة الإجرام المعلوماتي جديدة ومتجددة ، ولأن قطاع تكنولوجيات الاعلام ولاتصال في تطور مستمر، فهذا يعني أنه يمكن أن تظهر مستقبلا أنواع أخرى من الجرائم المعلوماتية ، مما يجعل المشرع الجزائري ملزم بمواكبة التطورات المتلاحقة عبر سن تشريعات زجرية جديدة أو تعديلات أخرى ،

وفي الأخير ، استطعنا أن نفرز جملة من الأفكار و المقترحات أهمها :

- على المشرع الجزائري أن يتدخل لمواجهة الجريمة المعلوماتية التي ترتكب للإعتداء على الاموال ، وهو مايتطلب ضرورة التنظيم القانوني للنقود الالكترونية بتعريفها ورسم الاطار القانوني الخاص بها وتحديد الجهات الوطنية المختصة باصدارها وطرحها للجمهور

---

[1] أنظر نص المادة 05 من قانون رقم 04 /09 المؤرخ في 05 أ،ت 2009 الموافق 16اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها ، ج،ر،ع47.

حتى يتسنى مواجهة الاحتيال والتلاعب بهذه الاموال ، والعمل على عقد اتفاقات دولية ثنائية من أجل تسليم المجرمين المعلوماتيين .

- يجب أن تعمل الدولة على تبني جهازا خاصا للخبرة الجنائية للجريمة المعلوماتية، متكونة من فرق متخصصة فنيا وتقنيا في المجال المعلوماتي، على أن يتم إعادة النظر في القواعد التقليدية للخبرة، لأن إثبات الجريمة المعلوماتية يتطلب قواعد خاصة للتعامل مع الأدلة في هذه الجرائم .
- ضرورة تأهيل رجال الشرطة والمحققين تأهيلا يستطيع معه كل منهم التعامل مع هذا النوع من الجرائم المستحدثة ، العمل على عقد المزيد من الندوات العلمية والمؤتمرات حول العلاقة بين المعلوماتية والقانون، وتبني خطة واسعة للتدريب ورفع مستوى الكفاءة المعلوماتية في القطاع الوظيفي للدولة، ودورات تدريبية مكثفة للقضاة ورجال النيابة العامة لرفع مستوى الكفاءة لديهم في استخدام المعلوماتية.

عن فعالية دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحتها في الجزائر

On the effectiveness of the role of the National Commission for the Prevention and Combating of Media Technologies in Algeria

د. بولقواس سناء
أستاذة محاضرة قسم أ
كلية الحقوق والعلوم السياسية
جامعة عباس لغرور خنشلة- الجزائر

مقدمة:

إن الجرائم المتصلة بتكنولوجيا الإعلام كما اصطلح عليها المشرع الجزائري، والتي عرفت بتسميات أخرى على غرار: جرائم المعلوماتية أو جرائم الحاسبات الإلكترونية، من الجرائم الحديثة النشأة ،ومرد ذلك أنها تتعلق بتكنولوجيات الإعلام، وقد أصبحت من المواضيع الأكثر انتشارا على المستوى الدولي وحتى الإقليمي والمحلي، أفرزتها الاستخدامات السلبية للتكنولوجيا، حتى أن بعض الباحثين يرون أن هذه الجرائم نتيجة حتمية لكل تقدم علمي، ومن هنا تتسم هذه الأخيرة بخصوصية تميزها عن غيرها من الجرائم الالكترونية.

أصبحت الجرائم المتصلة بتكنولوجيات الإعلام تفرز عديد التحديات الإجرائية وغيرها، لاسيما بمدى قبول الدليل الإلكتروني، الذي يتطلب تقنيات حديثة وخبراء في ذلك من جهة، ومن جهة أخرى مدى حجيته، وهو ما يختلف من نظام قضائي لآخر، ضف لذلك مدى اعتمادها على الإثبات العلمي، ومن هنا كان لزاما على الجزائر وغيرها من الدول إيجاد إطار قانوني متكامل يكافح هذه الجرائم، ويواكب أساليب وتقنيات الإجرام التي تستخدم فيها، انطلاقا من القانون رقم 04/09، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، للقانون رقم 07/18، المتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وهذا حماية للحياة الخاصة للأفراد، والحفاظ على سمعتهم وشرفهم وكرامة عائلاتهم، بحماية معطياتهم الشخصية، والذي يشترط الموافقة الصريحة للشخص المعني،

من أجل معالجة معطياته الشخصية،[1] فالتطور الهائل في مجال تكنولوجيات الاتصال والمعلوماتية لم يقتصر على الحقوق المالية فقط[2]...الخ.

على الرغم من أهمية وجود نصوص قانونية تجرم وتكافح الجرائم المتعلقة بتكنولوجيات الإعلام، إلا أن وجود سلطة أو جهاز أو هيئة تتولى مهمة الوقاية والمكافحة لهذه الجرائم أكثر من حتمية يمليها الواقع، وهو ما فعله المشرع الجزائري سنة 2015، بإنشائه لهيئة تتولى ذلك، نحاول من خلال هذه الورقة البحثية الإجابة عن الإشكالية التالية: ما مدى فعالية دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في الوقاية أولا؟ ثم مكافحة الجرائم المعلوماتية على اختلاف أنواعها؟

أولا: مفهوم الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

تقتضي منا دراستنا لفاعلية دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام في الجزائر، إبراز المقصود بهذه الجرائم فقها، وكذا التعريف الذي أورده المشرع الجزائري لها، والمصطلحات ذات الصلة بها، كما نبرز خصائصها وذلك على النحو التالي:

1. تعريف الجرائم المتصلة بتكنولوجيات الإعلام

لم يتفق فقهاء القانون الجنائي على استعمال تسمية موحدة للجرائم المتصلة بتكنولوجيات الاعلام، فقد استخدمت هنا تسميات كثيرة منها: الجريمة المعلوماتية، والجرائم الإلكترونية، وهناك من سماها جرائم إساءة استخدام تكنولوجيات المعلومات والاتصال، وهنا من سماها بجرائم الكمبيوتر، وهناك من اطلق عليها تسمية الجرائم المستحدثة...الخ،[3] هي تسميات عديدة لجرائم متصلة بتكنولوجيات الإعلام، فهي تعتمد على التقنية في تنفيذها أو في مساسها.

نبرز عددا من التعاريف التي أورت لها على النحو التالي:

---

[1]- العيداني محمد، يوسف زروق، " حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي"، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي تندوف، العدد الخامس، ديسمبر 2018، ص 115.

[2]- طباش عز الدين، " الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري دراسة في ظل قانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي"، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، العدد الثاني، ديسمبر 2018، ص 28.

[3]- عادل يوسف عبد النبي الشكري، " الجريمة المعلوماتية وأزمة الشرعية الجزائية"، مجلة مركز دراسات الكوفة، جامعة الكوفة، العراق،المجلد الأول، العدد السابع، 2008، ص 112.

عرفت الجريمة المعلوماتية بأنها:"سلوك غير شروع، عن إرادة جنائية، يقرر له القانون عقوبة أو تدبيرا احترازيا"، يعاب على التعريف أنه لم يبرز الاختلاف بين جرائم تكنولوجيات الإعلام والجرائم، وكذا خصوصيتها وحداثتها.[1]

عرفت أيضا بأنها:" سلوك سيء متعمد، يستهدف الإضرار بتقنية المعلومات، أو يستخدم المعلومات لإلحاق الضرر، أو ينتج عنه حصول أو محاولة حصول المجرم على فائدة لا يستحقها"،[2] وعرفها الفقيه الألماني Tiede Mann بأنها:" كل أشكال السلوك غير المشروع أو الضار بالمجتمع، الذي يرتكب باستخدام الحاسوب".[3]

من خلال التعاريف السابقة، يمكننا تعريف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بأنها:" أفعال مجرمة قانونا، أفرزها التطور الحاصل في تكنولوجيا المعلومات والاتصال، تمس أنظمة المعالجة الآلية للمعطيات، التي يتولى المشرع تحديدها في قانون العقوبات، كما تشمل أيضا كل الجرائم التي يكون ارتكابها من خلال منظومة معلوماتية، أو اتصالات إلكترونية بوسائط الكترونية".

عرف المشرع الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بأنها:" جرائم المساس بأنظمة المعالجة الآلية للمعطيات، المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الالكترونية".

يقصد بمنظومة معلوماتية المشار إليها سابقا حسب المشرع الجزائري:" أي نظام منفصل، أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات، تنفيذا لبرنامج معين".

كما حدد المشرع المقصود بمعطيات معلوماتية بأنها:" أي عملية عرض للوقائع أو المعلومات أو المفاهيم، في شكل جاهز للمعالجة داخل منظومة، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها".

---

[1] محروس نصار غايب، " الجريمة المعلوماتية"، مجلة التقني، هيئة التعليم التقني، العراق، المجلد الرابع والعشرين، العدد التاسع، 2011، ص 102.

[2] طالب محمد جواد عباس، عبد الجبار ضاحي عواد، " جرائم تقنية المعلومات وإثباتها"، مجلة كلية الرافدين للعلوم، كلية الرافدين الجامعة، العراق، العدد الثامن والعشرون، 2011، ص 5.

[3] سامية عبد الرزاق خلف، " جريمة اختراق أنظمة المعلومات (دراسة مقارنة)"، مجلة العلوم القانونية، جامعة بغداد، العراق، المجلد الخامس والعشرون، العدد لأول 2010، ص 283.

عرف المشرع الاتصالات الإلكترونية بأنها:" أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"،[1] عرفها أيضا بأنها:" كل تراسل أو إرسال أو استقبال علامات، أو إشارات أو كتابات أو صور أو أصوات أو معلومات، أيا كانت طبيعتها، عن طريق أي وسيلة إلكترونية، بما في ذلك وسائل الهاتف الثابت والنقال".[2]

2. خصائص الجرائم المتصلة بتكنولوجيات الإعلام[3]

تميز الجرائم المتصلة بتكنولوجيات الإعلام بعديد الخصائص نفصل فيها كالتالي:

- **صفة الجاني في جرائم المعلوماتية**

الجاني في الجرائم المتصلة بتكنولوجيات الإعلام قد يكون شخصا طبيعيا، ويعمل لحسابه ويسعى من اقترافها لتحقيق مصلحته الخاصة، من خلال اعتماده على نظم المعالجة الآلية للبيانات والمعلومات، لكن في الغالب ما يرتكب الشخص الطبيعي السلوك الإجرامي ليس لحسابه الخاص، وإنما لحساب شخص معنوي، عادة ما يكون شركة تعمل في ميدان المعلوماتية أو أي ميدان آخر.

- **الهدف من ارتكاب الجرائم المتصلة بتكنولوجيات الإعلام**

– **الدوافع الشخصية:** يمكن ارجاعها للسعي لتحقيق الربح، فالبحث عن الثراء الفاحش سبب لارتكاب الجريمة، كما أن ارتكابها قد يكون بسبب الرغبة في إثبات الذات، في الانتصار على الأنظمة المعلوماتية وإبراز قدراته في ذلك.

– **الدوافع الخارجية:** يمكن ارجاعها لاختصار عنصر الزمن، وتفادي استثمار مبالغ كبيرة في البحث العلمي، لذا تلجأ بعض المنشآت للتعامل مع أفراد في شركات ومؤسسات أخرى ليعملوا لصالحهم، والإطلاع على المعلومات والتقنيات المتوفرة لديها للاستفادة منها، من جهة أخرى قد يكون السبب راجعا لرغبة بعض الأشخاص في إظهار قدراتهم الفنية الكبيرة في مجال المعلوماتية،

---

[1]- المادة 2/أ، ب، ج، و، القانون رقم 04/09، المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 47.

[2]- المادة 1/5 من المرسوم الرئاسي رقم 261/15، المؤرخ في 8 أكتوبر 2015، المتضمن تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 53.

[3]- عادل يوسف عبد النبي الشكري، المرجع السابق، ص ص 114، 117.

للوصول لمركز أعلى في الشركة، وأخيرا قد يكون السبب الرغبة في الانتقام من المستخدم أو من أحد الزملاء.

- ارتكاب الجرائم المتصلة بتكنولوجيات الإعلام خلال مرحلة تشغيل نظام المعالجة الآلية للبيانات

على الرغم من إمكانية ارتكاب الجريمة المعلوماتية في أي مرحلة من مراحل تشغيل نظام المعالجة الآلية للبيانات، إلا أن لكل مرحلة منها نوعية خاصة من الجرائم، لكن جرائم الاتصال بتكنولوجيات الإعلام لا يمكن أن ترتكب إلا في مراحل التشغيل، لأنها المرحلة التي تترجم المعلومات فيها للغة مفهومة، وفيها ترتكب أغلبية الجرائم المتصلة بتكنولوجيات الإعلام، في مرحلة معالجة الآلية للبيانات فيمكن إدخال التعديلات على برامج الحاسوب، لتحقيق الأهداف الإجرامية عن طريق التلاعب ببرامج النظام المعلوماتي، وتتطلب الجرائم المرتكبة معرفة فنية كبيرة من الجاني في مجال التقنية.

- **وقوع الجريمة في بيئة المعالجة الآلية للبيانات والمعلومات:** لابد من وقوع الجريمة على بيانات مجمعة، ومجهزة للدخول للنظام المعلوماتي، من أجل معالجتها إلكترونيا، من خلال العمليات المتبعة التي تتوافر على إمكانية التعديل والتصحيح...الخ.

- **التعاون على الإضرار:** يكون متكررا بشكل كبير في الجرائم المعلوماتية، مقارنة بغيرها من الجرائم، فهذا النوع من هذه الجرائم يقوم بها متخصصون في مجال التقنية، بالتواطؤ مع آخرين قد يكونون في شركات منافسة، بتزويدهم بالمعلومات وتحويل مكاسب مالية.

- **صعوبة كشف وإثبات الجرائم المتصلة بتكنولوجيات الإعلام:** تتسم بصعوبة الإثبات لأنها متعلقة ببيانات ومعلومات يتم تغييرها، أو حتى محوها كليا أو جزئيا من ذاكرة الحاسوب، وإثباتها يتسم بالصعوبة لأنها لا تترك آثارا خارجية، فهي لا تتم بدليل كتابي وإنما باستخدام التقنية ونقل المعلومات، كما أنها تتسم بالصعوبة في الاحتفاظ الفني بآثارها ان وجدت،[1] ضف لذلك مرتكبوها خبراء في مجال المعلوماتية والحواسيب، ما يصعب على الجهات المختصة إثباتها.[2]

[1]- عمر طه خليل، عفاف بديع جميل، " التكييف الفقهي والقانوني لجرائم الإنترنيت"، مجلة كلية التراث الجامعة، كلية التراث الجامعة، العراق، العدد السابع عشرة، 2015، ص 167.

[2]- محمد علي سالم، حسون عبيد هجيج، " الجريمة المعلوماتية"، مجلة جامعة بابل، جامعة بابل، العراق، الجلد الرابع عشرة، العدد الثاني، 2007، ص 88.

- **سمات المجرم الالكتروني:** يتسم المجرم الالكتروني بصغر سنه، لأنه أكثر تعاملا مع الحاسوب، ويواكب التطورات في مجال التقنية، فهم متخصصون في هذا النوع من الجرائم،[1] كما أن مجرمي الجرائم الالكترونية يتسمون بالذكاء مقارنة بالمجرمين العاديين، الذين يتسمون بالعنف، كما أنهم مجرمون محترفون، وهم مجرمون دائما في حالة العود.[2]

ثانيا: دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحتها في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام

نص المشرع لأول مرة في القانون رقم 04/09، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، في الفصل الخامس على إنشاء جهاز تحت تسمية" الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته"، وأحالنا في تنظيمها للتنظيم الذي صدر بعد ذلك، نفصل في فاعلية دورها من خلال إبراز المهام الموكلة لها، وكذا طبيعتها القانونية على النحو التالي:

1. مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحتها

بين مهامها المشرع على سبيل المثال في القانون رقم 04/09، وهي:

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.
- مساعدة السلطات القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.
- تبادل المعلومات مع نظيراتها في الخارج، قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام، وتحديد مكان تواجدهم.[3]

بصدور المرسوم الرئاسي المنظم لتشكيلتها وسيرها، نص المشرع على تكليفها ما يلي:

- اقتراح عناصر الاستراتيجية الوطنية للوقاية، من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- تنشيط وتنسيق عمليات الوقاية، من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ومكافحتها.

---

[1]- مشتاق طالب وهيب، " مفهوم الجريمة المعلوماتية ودور الحاسوب بارتكابها"، مجلة العلوم القانونية والسياسية، جامعة ديالى، العراق، المجلد الثالث، العدد الأول، 2014، ص 352.

[2]- نفس المرجع، ص 92.

[3]- المادتين 13، 14 من القانون رقم 04/09، المشار إليه سابقا.

- مساعدة السلطات القضائية ومصالح الشرطة القضائية، في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.
- ضمان المراقبة الوقائية للاتصالات الإلكترونية، قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة، تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.
- تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها، ومسارها من أجل استعمالها في الإجراءات القضائية.
- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية، وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.
- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية، بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- المساهمة في تكوين المحققين المتخصصين، في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام.
- المساهمة في تحديث المعايير القانونية في مجال اختصاصها.[1]

2. الطبيعة القانونية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

حدد المشرع الجزائري الطبيعة القانونية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنها سلطة إدارية مستقلة، وقد نص على تمتعها بالشخصية المعنوية والاستقلال المالي، ونص على وضعها تحت الوزير المكلف بالعدل، وجعل مقرها الهيئة بمدينة الجزائر،[2] وهنا يطرح تساؤل عن مدى استقلاليتها؟ وهل يمكن للوزير المكلف بالعدل التدخل في مهامها؟

---

[1]- المادة 4 من المرسوم الرئاسي رقم 261/15، المشار إليه سابقا.

[2]- المادتين: 2، 3 من نفس المرسوم الرئاسي.

لقد ظهرت السلطات الإدارية المستقلة في الجزائر مع انسحاب الدولة من المجال الاقتصادي،[1] وكانت البداية بإنشاء المجلس الأعلى للإعلام سنة 1990،[2] تلته عديد السلطات الإدارية المستقلة، والتي تعد الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال أحدها حسب نص المادة السابق، وهو أمر إيجابي عموما، عوضا عن إيكال مهمة الرقابة للهيئات الإدارية التقليدية، لأن الأمر يعلق بوظيفة ضبط من جهة، ومن جهة أخرى هذا التكييف سيجعلها من المفروض لا تخضع لأي رقابة إدارية أو وصائية، ولا تخضع للتدرج الهرمي الذي تميز به الإدارة والهياكل المكونة لها.[3]

عدل المشرع من طبيعة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها سنة 2019، الأمر الذي يدل على تغير وجهة المشرع في التوسع في إنشاء السلطات الإدارية المستقلة، فقد حولها لمؤسسة عمومية ذات طابع إداري، فنص على أنه:" الهيئة مؤسسة عمومية ذات طابع إداري، تتمتع بالشخصية المعنوية والاستقلالية المالية، توضع تحت سلطة وزارة الدفاع الوطني"،[4] كما نص المشرع في المرسوم الرئاسي رقم 172/19، على إمكانية نقل مقر الهيئة لأي مكان من التراب الوطني، بموجب قرار من وزير الدفاع الوطني.[5]

3. تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

3-1: في ظل تكييفها كسلطة إدارية مستقلة

- **لجنة مديرة:** يترأسها الوزير المكلف بالعدل، وتضم كل من: الوزير المكلف بالداخلية، والوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال، وقائد الدرك الوطني، والمدير العام للأمن

---

[1]- نزليوي صليحة، " سلطات الضبط المستقلة: آلية للانتقال من الدولة المتدخلة إلى الدولة الضابطة"، مداخلة مقدمة للمشاركة في الملتقى الوطني الموسوم :" سلطات الضبط المستقلة في المجال الاقتصادي والمالي"، جامعة عبد الرحمن ميرة، بجاية، يومي 24/23 ماي 2007، ص 5.

[2]- القانون رقم 07/90، المؤرخ في 3 أفريل 1990، المتضمن الإعلام، ج ر عدد 14. **(ملغى)**

[3]- حدري سمير، " السلطات الإدارية المستقلة وإشكالية الاستقلالية"، مداخلة مقدمة للمشاركة في الملتقى الوطني الموسوم :" سلطات الضبط المستقلة في المجال الاقتصادي والمالي"، جامعة عبد الرحمن ميرة، بجاية، يومي 24/23 ماي 2007، ص 44.

[4]- المادة 2 من المرسوم الرئاسي رقم 172/19، المؤرخ في 6 يونيو 2019، المتضمن تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج ر عدد 37.

[5]- المادة 3 من نفس المرسوم الرئاسي.

الوطني، وممثل عن رئاسة الجمهورية، وممثل عن وزارة الدفاع الوطني، وقاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

يتم تعيين ممثلا رئاسة الجمهورية ووزارة الدفاع الوطني بموجب مرسوم رئاسي.

يلاحظ على تشكيلة اللجنة المديرة أنها:

✓ متنوعة فأعضاؤها من قطاعات مختلفة، الأمر الذي يراه الفقه ضمانة لاستقلالية السلطات الإدارية المستقلة، لكنها في نفس الوقت تحوي عددا من السلطة التنفيذية، الأمر الذي يؤثر على استقلاليتها في مهامها.

✓ عدم تحديد أساس الانتقاء بالنسبة للممثلين، وترك السلطة التقديرية لجهة التعيين.

✓ عدم تحديد مدة العهدة وعدم قابليتها للتجديد، وهي من الأمور المهمة لضمان استقلالية الهيئة.

تكلف اللجنة المديرة على وجه الخصوص بما يلي:

✓ توجيه عمل الهيئة والإشراف عليه ومراقبته، ودراسة كل مسألة تخضع لمجال اختصاص الهيئة، لاسيما فيما يتعلق بتوفير شروط اللجوء للمراقبة الوقائية للاتصالات الالكترونية.

✓ ضبط برنامج عمل الهيئة، وتحديد شروط وكيفيات تنفيذه، والقيام دوريا بتقييم حالة الخطر في مجال الإرهاب، والتخريب والمساس بأمن الدولة، للتمكن من تحديد مشتملات عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة.

✓ اقتراح كل نشاط يتصل بالبحث، وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

✓ دراسة كل من: مشروع النظام الداخلي للهيئة والموافقة عليه، ومشروع ميزانية الهيئة والموافقة عليه، والتقرير السنوي لنشاطات الهيئة والمصادقة عليه، نشير هنا إلى أن المشرع لم يبين من يتولى إعداد النظام الداخلي للهيئة، وهو في غاية الأهمية لأنه من مرتكزات الاستقلالية الوظيفية لها كسلطة إدارية مستقلة، خلافا لمشروع الميزانية الذي يضعه المدير العام.

✓ إبداء رأيها في كل مسألة تتصل بمهام الهيئة، وتقديم كل اقتراح مفيد يتصل بمجال اختصاص الهيئة.

- **مديرية عامة:** يتولى إدارتها مدير عام معين بموجب مرسوم رئاسي، وهذا فيه تأثير على استقلالية الهيئة، وتنهى مهامه تطبيقا لقاعدة توازي الأشكال بنفس الطريقة،[1] وتتكون من: أمانة

[1] المادة 9 من المرسوم الرئاسي رقم 261/15، المشار إليه سابقا.

عامة، ومصلحة الإدارة العامة، ومكتب الموارد البشرية، ومكتب المالية والوسائل، ومكتب الوقاية والأمن.[1]

أوكل المشرع المدير العام الصلاحيات التالية على سبيل المثال:

✓ السهر على حسن سير الهيئة، وعلى تنفيذ برنامج عمل الهيئة، وتنشيط نشاطات هياكل الهيئة وتنسيقها ومتابعتها ومراقبتها، واحترام قواعد حماية السر في الهيئة.

✓ تحضير اجتماعات اللجنة المديرة، وتمثيل الهيئة لدى السلطات والمؤسسات الوطنية والدولية، ولدى القضاء، وفي جميع أعمال الحياة المدنية.

✓ ممارسة السلطة السلمية على مستخدمي الهيئة، والسهر على القيام بإجراءات التأهيل وآداء اليمين فيما يخص المستخدمين المعنيين في الهيئة.

✓ إعداد التقرير السنوي لنشاطات الهيئة، وعرضه على اللجنة المديرة للمصادقة عليه.

✓ ضمان التسيير الإداري والمالي للهيئة.[2]

- **مديرية للمراقبة الوقائية واليقظة الالكترونية:** نص المشرع على إنشاء مركز العمليات التقنية وجعله تابعا لهذه المديرية، وجعل تشغيله يتم من قبلها، ونص على تزويده بالنظر لأهمية الدور الذي يؤديه، بالمنشآت والتجهيزات والوسائل المادية، وكذا بالمستخدمين التقنيين الضروريين لتنفيذ العمليات التقنية لمراقبة الاتصالات الإلكترونية.[3]

يعين مدير المراقبة الوقائية واليقظة الإلكترونية بموجب مرسوم رئاسي.[4]

جعل المشرع هياكل مديرية المراقبة والوقاية واليقظة الإلكتروني كالتالي:

- **مصلحة المراقبة الإلكترونية:** وفيها مكتب 3 مكاتب: مكتب تنسيق النشاطات، ومكتب مراقبة الاتصالات السلكية واللاسلكية، ومكتب مراقبة شبكة الإنترنيت.

- **مصلحة المتابعة والتحليل والتعاون:** تتكون من 3 مكاتب: مكتب جمع ومركزة استغلال المعلومات، مكتب الوقاية والمتابعة، مكتب الاتصال والتعاون.

---

[1]- المادتين 2، 3 من القرار الوزاري المشترك المؤرخ في 17 ديسمبر 2017، المتضمن التنظيم الداخلي لهياكل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 14.

[2]- المادة 10 المرسوم الرئاسي رقم 261/15، المشار إليه سابقا.

[3]- المادة 13 من نفس المرسوم الرئاسي.

[4]- المادة 37 من نفس المرسوم الرئاسي.

- **مركز العمليات التقنية والملحقات الجهوية:** فيه **مركز العمليات التقنية:** وفيه مكتب أنظمة مراقبة الانترنيت، مكتب أنظمة التموقع الجغرافي ومراقبة الاتصالات عبر الأقمار الصناعية، مكتب أنظمة المراقبة الهاتفية، مكتب الدعم التقني.

الملحقة الجهوية: فيها مكتب الإدارة العامة، ومكتب المراقبة الالكترونية، ومكتب المتابعة والتحليل ومكتب العمليات التقنية.

كلفها المشرع بالقيام بالمهام المبينة أدناه على سبيل المثال:

- تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية، للكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بناء على رخصة مكتوبة من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول.
- إرسال المعلومات المحصل عليها لسلطة القضائية ومصالح الشرطة القضائية المختصة.
- تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة، وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي هذه الجرائم والتعرف عليهم.
- جمع ومركزة واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- تنظيم و/أو المشاركة في عمليات التوعية حول استعمال تكنولوجيات الإعلام والاتصال، وحول المخاطر المتصلة بها.
- تنفيذ توجيهات اللجنة المديرة.
- تزويد السلطات القضائية ومصالح الشرطة القضائية، تلقائيا أو بناء على طلبها، بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال.
- وضع مركز العمليات التقنية والملحقات الجهوية قيد الخدمة والسهر على حسن سيرها، وكذا الحفاظ على الحالة الجيدة لمنشآتها وتجهيزاتها ووسائلها التقنية.
- تطبيق قواعد الحفاظ على السر في نشاطاتها.[1]
- **مديرية للتنسيق التقني:** يعين مدير التنسيق التقني بموجب مرسوم رئاسي.[2]

تتكون من: **مصلحة الدراسات والخبرات القضائية:** وفي 3 مكاتب، مكتب قاعدة المعطيات التحليلية، ومكتب الدراسات والإحصائيات، ومكتب التقنيات الرقمية والخبرات القضائية.

---

[1]- المادة 11 من المرسوم الرئاسي رقم 261/15، المشار إليه سابقا.

[2]- المادة 37 من نفس المرسوم الرئاسي.

مصلحة منظومة الإعلام: تتكون من 3 مكاتب: مكتب إدارة شبكة الإعلام الآلي، ومكتب الأبحاث والتطوير، ومكتب أمن منظومة الإعلام.[1]

كلفها المشرع على وجه الخصوص بما يلي:

✓ إنجاز الخبرات القضائية في مجال اختصاص الهيئة، وتكوين قاعدة معطيات تحليلية للإجرام المتصل بتكنولوجيات الإعلام والاتصال واستغلالها.

✓ إعداد الإحصائيات الوطنية المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

✓ القيام بمبادرة منها أو بناء على طلب اللجنة المديرة، بكل دراسة أو تحليل أو تقييم يتعلق بصلاحياتها، وتسيير منظومة الإعلام للهيئة وإدارتها.[2]

- **مركز للعمليات التقنية.**

- **ملحقات جهوية:** يتم تشغيلها من طرف مديرية المراقبة الوقائية واليقظة الإلكترونية التي تتبعها.[3]

الملاحظ على التنظيم الهيكلي للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أنه متنوع وراعى فيه المشرع طابع الجرائم محل اختصاصها، وحاجتها لتخصصات ومكاتب مختلفة، بهدف الوقاية منها أولا ثم مكافحتها ثانيا، من جهة أخرى هذا التنوع والتوزيع في الاختصاصات على هياكلها، هو ضمانة لنقل المعلومات ومعالجتها ولسرعة اتخاذ القرار بشأنها، ماعدا ذلك من أعمال إدارية فهو متروك للمصالح الإدارية والتقنية.

الملاحظ هنا فيما يتعلق بالاستقلالية العضوية للهيئة، على الرغم من اعتراف المشرع بذلك بنص صريح كما سبق الإشارة، إلا أنها محدودة لأنها:

- موضوعة لدى الوزير المكلف بالعدل، حسب نص المادة 2 من المرسوم الرئاسي رقم 261/15 المشار إليه سابقا.

- لا يوجد تعدد واختلاف في الجهات المقترحة لأعضائها، ولا على أي أساس يختارون، وفي الغالب ما يكون التعيين في يد جهة واحدة.

- تعيين ممثل رئاسة الجمهورية ووزارة الدفاع بموجب مرسوم رئاسي.

---

[1] - المواد: 9، 10، 11 من القرار الوزاري المشترك المؤرخ في 17 ديسمبر 2017، المشار إليه سابقا.

[2] - المادة 12 من المرسوم الرئاسي رقم 261/15، المشار إليه سابقا.

[3] - المادة 14 من نفس المرسوم الرئاسي.

- وجود وزيرين في اللجنة المديرة للهيئة (الوزير المكلف بالداخلية، الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال) .
- المديرية العامة يديرها مدير عام معين بموجب مرسوم رئاسي.
- مدير التنسيق التقني يعين بموجب مرسوم رئاسي.

3-2: في ظل تكييفها كمؤسسة عمومية ذات طابع إداري

بتغيير المشرع لتكييف الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جاء بتنظيم هيكلي جديد لها، لا يشابه ما هو موجود في المؤسسات العمومية ذات الطابع الإداري المعروفة، لا في تشكيلته ولا في المهام الموكلة لكل جهاز، كما أن السلطة الرقابة السلمية والوصائية لم تبرز بشكل واضح، وإن كانت نتيجة حتمية لهذا التكييف، ضف لذلك لم تعد للهيئة سلطة اقتراح مشاريع قوانين ونصوص تنظيمية في مجال اختصاصها، نفصل في هياكلها والمهام الموكلة له على النحو التالي:

أ. مجلس التوجيه

مجلس التوجيه يترأسه وزير الدفاع الوطني أو ممثله، وقد حدد المشرع تشكيلته فيما يلي:

- وزارة الدفاع الوطني- وزارة العدل -الوزارة المكلفة بالداخلية - الوزارة المكلفة بالمواصلات السلكية واللاسلكية.

تتولى المديرية العامة أمانة المجلس.[1]

المهام الموكلة لمجلس التوجيه:

- التداول حول الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وكذا حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- القيام دوريا بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، للتمكن من تحديد مضامين عمليات المراقبة الواجب القيام بها، والأهداف المنشودة بدقة.
- اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة، في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- الموافقة على برنامج عمل الهيئة، وإعداد نظامه الداخلي والمصادقة عليه أثناء أول اجتماع له.

---

[1]- المادتين 4، 5 من المرسوم الرئاسي رقم 172/19، المشار إليه سابقا.

- دراسة التقرير السنوي لنشاطات الهيئة والمصادقة عليه، وكذا دراسة مشروع ميزانية الهيئة والموافقة عليه.
- إبداء رأيه في كل مسألة تتصل بمهام الهيئة، وكذا تقديم كل اقتراح يتصل بمجال اختصاص الهيئة.
- المساهمة في ضبط المعايير القانونية في مجال اختصاصه. [1]

يجتمع مجلس التوجيه في دورة عادية مرتين في السنة، بناء على استدعاء من رئيسه، كما يمكن أن يجتمع في دورة غير عادية كلما كان ذلك ضروريا، بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة.[2]

ب. المديرية العامة

يتولى إدارة المديرية العامة مدير عام، وكلفه المشرع على سبيل المثال لا الحصر:

- السهر على حسن سير الهيئة. - إعداد مشروع ميزانية الهيئة.
- إعداد وتنفيذ برنامج عمل الهيئة. - تنشيط وتنسيق ومتابعة ومراقبة أنشطة هياكل الهيئة.
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- تبادل المعلومات مع مثيلاتها الأجنبية، بغرض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والتعرف عليهم.
- تحضير اجتماعات مجلس التوجيه. -إعداد التقرير السنوي لنشاطات الهيئة.

جعل المشرع المدير العام الآمر بالصرف ميزانية الهيئة.[3]

تتشكل هياكل المديرية العامة من: مديرية تقنية، ومديرية للإدارة والوسائل، ومصالح.

مهام مديرية التقنية:

- المراقبة الوقائية للاتصالات الالكترونية للوقاية من الموصوفة بالأفعال الارهابية والتخريبية والاعتداء على أمن الدولة.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية بناء على طلبها، بما في ذلك في مجال الخبرات القضائية، في إطار مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والجرائم التي تتطلب اللجوء إلى أساليب التحري الخاصة للهيئة.

---

[1]- المادة 6 من نفس المرسوم الرئاسي.
[2]- المادة 7 من نفس المرسوم الرئاسي.
[3]- المادة 9 من نفس المرسوم الرئاسي.

- جمع وتسجيل وحفظ المعطيات الرقية، وتحديد مصدرها، وتتبعها بغرض استعمالها في الاجراءات القضائية.

تمارس المديرية التقنية مهامها المرتبطة بالشرطة القضائية، وفقا لأحكام قانون الإجراءات الجزائية، وتتولى وضع التجهيزات والوسائل والأجهزة التقنية الضرورية لتنفيذ مهامها، على مستوى المنشآت القاعدية للمتعاملين ومقدمي الخدمات.[1]

مهام مديرية الإدارة والوسائل: تتولى بشكل خاص بما يلي:

- تسيير الموارد البشرية والوسائل والمالية الخاصة بالهيئة -الإسناد التمويني والإسناد التقني للهيئة.
- صيانة العتاد والوسائل والمنشآت القاعدية. - إعداد احتياجات الهيئة في إطار تحضير تقديرات الميزانية.[2]

4. التنظيم القانوني لعمل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

يكون اجتماع الهيئة المديرة بناء على استدعاء من رئيسها، أو بناء على طلب أحد أعضائها، وقد منحها المشرع سلطة إعداد نظامها الداخلي وتصادق عليه.

نص المشرع على تزويد الهيئة بقضاة وفقا لما هو محدد في التشريع، كما تزود بضباط وأعوان للشرطة القضائية من المصالح العسكرية للاستعلام، والأمن والدرك الوطني والأمن الوطني، أما عددهم فقد أحالنا المشرع للقرارات المشتركة، التي تكون بين الوزراء المكلفين بالعدل والدفاع الوطني والأمن الوطني، أي أن الهيئة لا تمتع باستقلالية في ذلك ومرد ذلك تعلقها بمصالح عسكرية، ونص على تزويدها أيضا بمستخدمي الدعم التقني والإداري، ويجلبون من ضمن مستخدمي المصالح العسكرية للاستعلام، والأمن والدرك الوطني والأمن الوطني.[3]

لتتمكن الهيئة من تأدية مهامها، نص المشرع على تمكينها من الاستعانة بكل خبير أو شخص يمكن أن يساعدها في القيام بمهامها،[4] وأكثر من ذلك مكنها من:

✓ طلب أي وثيقة أو معلومة ضرورية، لإنجاز المهام المسندة لها، من أي جهاز أو مؤسسة أو مصلحة.

---

[1]- المواد: 11، 12، 13، 14 من نفس المرسوم الرئاسي.

[2]- المادة 15 من نفس المرسوم الرئاسي.

[3]- المادتين 16، 17، 18 من المرسوم الرئاسي رقم 261/15، المشار إليه سابقا.

[4]- المادة 19 من نفس المرسوم الرئاسي.

تأليف مجموعة من الباحثين

✓ مراقبة الاتصالات الإلكترونية، وتجميع وتسجيل محتواها في حينها، والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية، تحت سلطة قاض مختص، للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة.

✓ وضع وحدة مراقبة واحدة أو أكثر، تزود بالوسائل والتجهيزات التقنية الضرورية، مكونة من مستخدمين تقنيين يعملون تحت إدارة ومراقبة قاض، يساعده ضابط واحد من ضباط الشرطة القضائية أو أكثر ينتمي للهيئة، وتتولى تحرير محاضر بالأشغال التي تقوم بها، وفي كل الحالات لا يمكن أن يشارك في عملية المراقبة للاتصالات الالكترونية، إلا أعضاء الوحدة أو الوحدات التي أوكلت لها السلطة القضائية هذه المهمة، ويتخذ مسؤول الوحدة أثناء سير العملية، كل التدابير اللازمة بالاتصال مع المسؤولين المعنيين في الهيئة، من أجل ضمان سرية العملية وحماية المعلومات المستقاة من المراقبة.[1]

الملاحظ هنا أن الأحكام الخاصة بهذه الهيئة سواء عند تكييفها كسلطة إدارية مستقلة أو بعد تكييفها كمؤسسة عمومية ذات طابع إداري، ففي الحالة الأولى كانت سلطة مختلفة عن باقي السلطات الإدارية المنشأة، والأمر سيان في الحالة الثانية.

تحفظ المعلومات المتحصل عليها أثناء عمليات المراقبة، خلال حيازتها من الهيئة وفقا للقواعد المطبقة على حماية المعلومات المصنفة، كما أن تسجيل الاتصالات الالكترونية موضوع مراقبة، يحرر وفقا للشروط والأشكال المنصوص عليها في قانون الإجراءات الجزائية، وتسلم التسجيلات والمحررات للسلطات القضائية، ولمصالح الشرطة القضائية المختصة، ويكون الاختصاص بالاحتفاظ بهذه المعطيات أثناء المدة القانونية المنصوص عليها في التشريع اختصاصا حكريا للسلطات القضائية، وكل استخدام لتلك المعلومات لأغراض غير تلك التي تتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يكون تحت طائلة العقوبات الجزائية، ولضمان الحفاظ على السر المهني ألزم المشرع مستخدمي الهيئة بالسر المهني وواجب التحفظ، وكل ستخدمي الهيئة الذين يدعون للإطلاع على المعلومات السرية يؤدون يمينا أمام المجلس قبل تنصيبهم.[2]

إرسال التقارير

---

[1]- المواد: 20، 21، 22، 23 من نفس المرسوم الرئاسي.

[2]- المواد: 24، 25، 26، 27 من نفس المرسوم الرئاسي.

يقوم رئيس اللجنة المديرة للهيئة بإرسال تقارير فصلية لرئيس الجمهورية عن نشاطات الهيئة،[1] ويعد هذا من أهم القيود التي ترد على الاستقلالية الوظيفية للسلطات الإدارية المستقلة، والذي يرسل للسلطة التنفيذية وهنا في مجال دراستنا لرئيس الجمهورية.

5. ميزانية الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

يتم إعداد الميزانية من طرف المدير العام، ثم يعرضها على اللجنة المديرة للموافقة عليها، وتسجل ميزانيتها في الميزانية العامة للدولة، والأمر بالصرف هو المدير العام.[2]

تسجيل ميزانية الهيئة في الميزانية العامة للدولة نتيجة حتمية في ظل إيراداتها هي إعانات من الدولة فقط، لذا كنتيجة حتمية فمسك محاسبتها يتم وفقا لقواعد المحاسبة العمومية، والمراقبة المالية للهيئة يمارسها مراقب يعينه الوزير المكلف بالمالية،[3] والاستقلالية المالية للسلطة الإدارية المستقلة من أهم ركائز الاستقلالية الوظيفية، وقد كرسه المشرع للهيئة، لكن مادامت تحصل على إعانات من الدولة، فلا مجال للحديث عن استقلالية مالية لها، ومن ثم فهي خاضعة للرقابة.

في ظل المرسوم الرئاسي 172/19، عدل المشرع عن المصدر الواحد في إيرادات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بإضافة مورد جديد وهي عائدات كل النشاطات المرتبطة بموضوعها في المادة 1/16 منه، وأبقى المشرع على مسك محاسبتها حسب قواعد المحاسبة العمومية فهي مؤسسة عمومية ذات طابع إداري،[4] ومن هنا تبقى خاضعة لكل أنواع المراقبة المنصوص عليها قانونا.[5]

نشير إلى أن أسلوب المؤسسة العامة سيجعل من هذه الهيئة تمتع بموارد مالية وتكنولوجية، وأعداد كبيرة من الموظفين في اختصاصات متعددة، لكن من جهة أخرى فالدراسات في مجال المؤسسات العامة، تشير إلى أنه يمكن أن تكون بسبب هذه الموارد الضخمة وخصائص الرقابة التي تمارسها الدولة عليها، جعل الدولة في أغلب الدول تتحول لمجموعة من المؤسسات البيروقراطية،

---

[1]- المادة 32 من نفس المرسوم الرئاسي.

[2]- المادة 33 من نفس المرسوم الرئاسي.

[3]- المواد: 34، 35، 36 من نفس المرسوم الرئاسي.

[4]- المادة 17 من المرسوم الرئاسي رقم 172/19، المشار إليه سابقا.

[5]- المادة 18 من نفس المرسوم الرئاسي.

والتي تتسم بعدم الكفاءة وسوء استخدام الموارد والبطء في الإجراءات،[1] الأمر الذي نراه سينعكس سلبا على فعالية دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام في الجزائر، خاصة وأن:

- المؤسسات العمومية هي رسمية وتحد من الكفاءة والفاعلية.
- تفتقر لقدر ملائم للتنسيق، وتقوم على سلطة أحادية الجانب ضمن سلطة هرمية.
- الموظفون يركزون على النفقات، دون التكاليف ومنافع لبرامج المسطرة.
- هي موجهة نحو تقييد العمل، بدلا من التوجه لرسالة المؤسسة العمومية.[2]

الخاتمة:

في ختام دراستنا توصلنا لجملة من النتائج والاقتراحات نوجزها فيما يلي:

أولا: النتائج

1. إنشاء المشرع لهذه الهيئة ليس مفاجئا، وإنما هو انعكاس لما هو موجود في الواقع العملي من تفشي سريع للجرائم المتصلة بتكنولوجيات الإعلام فيها، ومن ثم ضرورة إيجاد سلطة أو هيئة مختصة تتولى مساعدة الدولة في مهمة التنظيم والوقاية، ومكافحة هذه الجرائم الحديثة.

2. تحول المشرع في تكييف الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحته من طابع السلطة الإدارية المستقلة، لمؤسسة عمومية ذات طابع إداري، الأمر الذي سيجعل من مكافحة هذه الجرائم يتسم بالرتابة، بسبب البيروقراطية الإدارية ومختلف أنواع الرقابة التي تخضع لها المؤسسات العمومية الإدارية.

ثانيا: الاقتراحات

نرى أن تكييف السلطة الإدارية المستقلة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام ومكافحتها، أكثر فاعلية في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام مع ضرورة ضمان ما يلي في النصوص المنظمة لها:

---

[1]- نجم عبود نجم، " التحول إلى المؤسسات العامة القائمة على إدارة المعرفة المطالب الأساسية وتوقعات الأداء"، مجلة دفاتر اقتصادية، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة زيان عاشور، الجلفة، المجلد الثاني، العدد الرابع، سبتمبر 2012، ص 11.

[2]- نفس المرجع، ص 11.

- الطابع الجماعي للهيئة، وذلك لضمان كفاءة أدائها لمهامها في مجال الوقاية ومكافحة الجرائم المتصلة بتكنولوجيات الإعلام.
- تخصصية أعضاء الهيئة، وتدريبهم لضمان كفاءتهم ومواكبة التطورات الحاصلة في مجال الجرائم المتصلة بتكنولوجيات الإعلام.
- توافرها على هياكل متنوعة، كما فعل سابقا سيسمح بتكفلها بكل ما يدخل في اختصاصاتها سواء كانت استشارية أو رقابية.
- إيجاد أحكام خاصة بتحديد مدة انتداب رئيس الهيئة وأعضائها، لأن هذا مؤشر على استقلالية السلطات الإدارية المستقلة من الناحية العضوية، وضرورة النص على عدم قابلية العهدة للتجديد.
- النص على تولي الهيئة إعداد نظامها الداخلي والمصادقة عليه بعيدا عن تدخل السلطة التنفيذية فيه.
- عدم احتكار سلطة التعيين في الهيئة من قبل السلطة التنفيذية.
- التوسع في الصلاحيات الممنوحة للهيئة الاستشارية والرقابية والقمعية أيضا، باعتبار مهمتها الوقاية أولا ثم المكافحة ثانيا.
- ضمان استقلالية مالية فعلية للهيئة، فالإعانات المالية التي قد تحصل عليها من الدولة سبب في عدم استقلاليتها وخضوعها للرقابة.
- الاطلاع على التشريعات المقارنة والاستفادة من تجاربها، في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام في مجال الهيئات التي تنشئها لهذا الغرض.

الحماية الدولية للملكية الفكرية في البيئة الرقمية على ضوء إتفاقية الويبو 1996.

International protection of intellectual property in the digital environment in the light of the WIPO Convention 1996.

عليلي أسامة باحث دكتوراه
معهد الحقوق و العلوم السياسية
المركز الجامعي مغنية – تلمسان- الجزائر

مقدمة:

إن الثورات المعرفية والعلمية التي شهدتها مختلف مجالات العلوم، وبالأخص في الجانب التكنولوجي ووسائل الإتصال الحديث السلكية واللاسلكية منها، كأجهزة الكمبيوتر والهواتف النقالة الذكية وكذا كل ما يتصل بالشبكة العنكبوتية العالمية، باعتبار أن هذه الوسائل الحديثة التي عرفتها المجتمعات لم تكن متداولة فيما سبق، مما تمّخض عن سوء استخدامها مساس بحقوق وحريات الآخرين وهو مايشكّل جريمة في مفهوم القانون الجنائي[1]، الأمر الذي حتم على الدول والمجتمعات تنظيم هذا المجال وتأطيره بموجب قوانين وأنظمة واتفاقات إقليمية ودولية[2].

وبعد تأسيس المنظمة العالمية للملكية الفكرية (الويبو) في ستوكهولم سنة 1967 عملت هذه الأخيرة على تشجيع النشاط الفكري وتيسير نقل التكنولوجيا المرتبطة بالملكية الصناعية إلى البلدان النامية؛ فبالرغم من أنّ إتفاقية تريبس جاءت شاملة للعديد من القضايا التي يثيرها التطور الجديد في مجال استعمال التكنولوجيا الرقمية ولا سيما عن طريق الإنترنت.

---

[1] - حاول المشرع الجزائري على غرار بقية التشريعات الوطنية معالجة هذه الظاهرة وتنظيمها بموجب قوانين منها ما هو خاص بما يتعلق بجانب الاتصالات كالقانون رقم 04/09 المؤرخ في 14 شعبان 1430 الموافق لـ 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج، ر، عدد 47 الصادر بتاريخ 16 أوت 2009؛ ومنها ما هو تحديث ومواكبة للقانون الجنائي الجزائري (قانون العقوبات وقانون الإجراءات الجزائية) كالقانون رقم 02/16 المؤرخ في 19 جوان 2016 المتمم للأمر 156/66 المتضمن قانون العقوبات، ج، ر، رقم 37 بتاريخ 22 جوان 2016.

[2] - محمد السعيد زناتي،(الجريمة المعلوماتية في ظل التشريع الجزائري والإتفاقيات الدولية)، مجلة إيليزا للبحوث والدراسات، العدد الثاني، المركز الجامعي إيليزي، الجزائر، 2017، ص ص 28-29.

إلا أن هذه الاتفاقية لم تتصدى لبعض تلك المسائل على نحو مفصل، الأمر الذي أدّى بالمنظمة العالمية للملكية الفكرية[1]إلى مواجهة هذا التحدي وذلك بإبرام معاهدتين في 20 ديسمبر 1996، وهما معاهدة الويبو بشأن حق المؤلف (المعاهدة الأولى) [2]، ومعاهدة الويبو بشأن الأداء والتسجيل الصوتي (المعاهدة الثانية)[3] ، والتي أطلق عليهما معاهدتا الإنترنت بالنظر لأهميتهما التي تتمثل فيما حملته أحكامهما من حلول للتحديات التي تطرحها التكنولوجيا الرقمية[4].

وتظهر أهمية هذا الموضوع إلى أن حق المؤلف يمكن أن يكون عنصرا محركا في الإقتصاديات الوطنية والدولية ،إذ تعتبر قضية حماية الملكية الفكرية وبالتحديد حماية المصنفات الأدبية والفنية عبر شبكة الإنترنت من أهم التحديات التي تواجهها التشريعات في الوقت الحاضر والتي تتطلب إيجاد حلول لها قابلة للتنفيذ.

وفي هذا الصدد ،ومن خلال الطرح السالف الذكر، إرتأينا إلى طرح إشكالية الدراسة التالية:

ماهي الضمانات التي تقدمها إتفاقية الويبو لسنة 1996 لحماية الملكية الفكرية في البيئة الرقمية؟

وللإجابة على إشكالية الدراسة، إرتأينا تقسيك الدراسة إلى محورين:

المحور الأول: حماية حق المؤلف في إطار إتفاقية الإنترنت الأولى.

المحور الثاني: القواعد الحمائية للملكية الفكرية في إطار إتفاقية الإنترنت الثانية.

المحور الأول: حماية حق المؤلف في إطار إتفاقية الإنترنت الأولى

---

[1] - صادقت الجزائر على إتفاقية إنشاء منظمة التجارة العالمية للملكية الفكرية الموقعة بـ استوكهولم في 14 جويلية 1967، بموجب الأمر رقم 02/75 المؤرخ في 09 جانفي 1975، مؤرخة في 14 فيفري 1975، عدد 13، ص 198.

[2] - إتفاقية الإنترنت الأولى (الويبو الأولى) بشأن حق المؤلف، وهي إتفاق خاص في إطار إتفاقية برن وتتناول حماية المصنفات وحقوق مؤلفيها في البيئة الرقمية، تمّ اعتمادها بتاريخ 20 ديسمبر 1996.

[3] - إتفاقية الإنترنت الثانية (الويبو الثانية) بشأن الأداء والتسجيل الصوتي، وتتناول حقوقا لنوعين من المستفيدين ولا سيما في البيئة الرقمية هما: " فنانو الأداء ومنتجو التسجيلات الصوتية"، تم اعتمادها بتاريخ 20 ديسمبر 1996.

[4] صلاح زين الدين، المدخل إلى الملكية الفكرية: نشأتها ومفهومها ونطاقها وأهميتها وتكييفها وتنظيمها، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2006، ص 174.

إنّ التطور التكنولوجي في المجال المعلوماتي والإتصال وأثر ذلك على إبتكار المصنفات الأدبية والفنية والإنتفاع بها وتحويل المؤلفات التقليدية ونتاج الأفكار لتوضع في فضاء الإنترنت مما ينعكس على الحماية الممنوحة بموجب حق المؤلف.

ونظرا لإستخدام شبكة الإنترنت والتي تحتوي على الملايين من المواقع التي تتضمن محركات للبحث ومصنفات رقمية ،الأمر الذي أدى إلى ظهور إشكالات قانونية متعددة كما أثّر كذلك على حماية المصنفات الأدبية والفنية ،هذه العوامل تجلت بظهور إتفاقية المنظمة العالمية للملكية الفكرية بشأن حق المؤلف (معاهدة الإنترنت الأولى) لتحقق كل هذه المتطلبات.

وفي هذا الصدد سنقوم بتبيان نطاق الحماية المقرّرة **(أولا)**، ثم نبين أثار الحماية من خلال الحقوق والإلتزامات التي رتبتها هذه الإتفاقية **(ثانيا)**.

أولا:نطاق الحماية المقررة في ظل إتفاقية الإنترنت الأولى

توجب إتفاقية الويبو على الدول الأطراف ضرورة النص في قوانينها الداخلية على حماية حقوق المؤلف على شبكة الإنترنت، كما حددت نطاق حماية حق المؤلف، حيث حاولت أن تتلاءم مع القواعد العامة الواردة في إتفاقية برن، حيث شملت حقوق التأليف التي تم التعبير عنها على الموقع الإلكتروني دون الأفكار أو الإجراءات أو أساليب العمل أو مفاهيم الرياضيات في حد ذاتها، والتي لم يتم التعبير عنها بشكل ملموس في الموقع الّإلكتروني.

ويمتد نطاق الحماية كذلك ليشمل برامج الحاسب الآلي باعتبارها مصنفات أدبية، وعليه فإن برامج الحاسب الآلي الموضوعة في الموقع الإلكتروني تمتع بذات الحماية المقررة للبرامج المخزنة في القرص المدمج[1].

كما اشتمل نطاق الحماية قواعد البيانات أيا كان شكلها وفقا لنص المادة 13، إذا كانت تعتبر إبتكارات فكرية بسبب اختيار محتوياتها أو ترتيبها في شكل ابتكار معين.

---

[1] - بقنيش عثمان ،مصطفى هنشور وسيمة، حماية الملكية الفكرية عبر الإنترنت في إطار المنظمة العالمية للملكية الفكرية، مجلة البحوث في الحقوق والعلوم السياسية ،العدد02 ،بدون سنة النشر ،ص 367.

وقد أكدت المادة 13 من الإتفاقية[1]على ضرورة تطبيق أحكام المادة 18 من اتفاقية برن[2] على كل أوجه الحماية المنصوص عليها فيها، فمدة الحماية الممنوحة للمؤلفين بناء على هذه الإتفاقية تسري حتى نهاية مدة خمسين سنة على الأقل[3].

وتبين الإتفاقية موضوعين يتعين حمايتهما بموجب حق المؤلفوهما:

- برامج الحاسوب أيا كانت طريقة التعبير عنها أو شكلها ، وتعرف بأنها: " مجموعة من التعليمات الموجهة من الإنسان إلى الآلة التي تسمح بتنفيذ مهمة معينة "[4].

مجموعة البيانات أو المواد الأخرى (قواعد البيانات) أيا كان شكلها ،إذا كانت تعتبر إبتكارات فكرية بسبب إختيار محتوياتها أو ترتيبها.(ولا تدخل في نطاق الإتفاقية أية قاعدة للبيانات لا تعد بمثابة إبتكار من ذلك القبيل)[5].

ثانيا: أثار الحماية المقررة على ضوء إتفاقية الإنترنت الأولى لسنة 1996

[1] - تنص المادة 13 من إتفاقية الإنترنت الأولى بشأن حق المؤلف لسنة 1996 على ما يلي: "تطبق الأطراف المتعاقدة أحكام المادة 18 من إتفاقية برن على كل أوجه الحماية المنصوص عليها في هذه المعاهدة".

[2] - إتفاقية برن لحماية المصنفات الأدبية والفنية وهي إتفاقية عالمية تعنى بحماية الحقوق الفكرية للمؤلفين وغيرهم، انعقدت لأول مرة في برن بسويسرا سنة 1886، تم التوقيع عليها بتاريخ 09 سبتمبر 1886، ودخلت حيز النفاذ بتاريخ 05 ديسمبر 1887. وقد تمّ تعديلها في عدّة مؤتمرات وكانت آخر نسخة إعتُمدت في باريس بتاريخ 28 سبتمبر 1979، صادقت عليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم 341/97 المؤرخ في 13 سبتمبر 1997، ج، ر، مؤرخة في 14 سبتمبر 1997، عدد 61، ص 08.

وتنص المادة 18 منها على ما يلي: "المصنفات الموجودة عند دخول الإتفاقية حيز التنفيذ(1) يجوز حمايتها في حالة عدم إنقضاء مدة الحماية في دولة المنشأ(2) لايجوز حمايتها في حالة إنقضاء مدة الحماية في الدولة المطلوب توفير الحماية فيها (3) تطبيق هذه المبادئ (4) حالات خاصة ".

[3] - بن ديدي جميلة، (الحماية الوطنية والدولية للمصنفات الأدبية)، مذكرة مكملة لنيل شهادة الماجستير في الحقوق تخصص قانون الملكية الفكرية ، كلية الحقوق والعلوم السياسية ،جامعة الحاج لخضر - باتنة1 - 2016/2015، ص 156.

[4] - بقنيش عثمان ،مصطفى هنشور وسيمة، (حماية الملكية الفكرية عبر الإنترنت في إطار المنظمة العالمية للملكية الفكرية)، مجلة البحوث في الحقوق والعلوم السياسية ،العدد02 ، بدون سنة النشر ،ص 396.

[5] - تشمل (قواعد البيانات) النصوص ،الصور والأصوات المحفوظة رقميا والتي بذل فيها جهد فكري ومادي في جمعها وتنسيقها ،ويتم تخزينها ويمكن إسترجاعها والإستفادة منها عند الحاجة.أنظر، بقنيش عثمان، مصطفى هنشور، وسيمة، مرجع سابق، ص364.

يترتب على الحماية الممنوحة بموجب إتفاقية الويبو بشأن حق المؤلف لسنة 1996 حقوق والتزامات على عاتق الأطراف لمتعاقدة.

أ- الحقوق المضمونة بموجب هذه إتفاقية الويبو

وتمثل هذه الحقوق في التالي:

1- حق التوزيع والتأجير

يتمتع مؤلفو المصنفات الأدبية والفنية بالحق الإستئثاري في التصريح بإتاحة النسخة الأصلية أو غيرها من نسخ مصنفاتهم للجمهور ببيعها أو نقل ملكيتها بطريقة أخرى ،ولا تؤثر هذه الإتفاقية في حرية الأطراف المتعاقدة في تحديد أي شروط في إستنفاذ الحق المذكور آنفا بعد بيع النسخة الأصلية أو غيرها من نسخ المصنف أو نقل ملكيتها بطريقة أخرى للمرة الأولى بتصريح المؤلف[1].

هذا يعني أن لمؤلفي برامج الحاسوب التي وضعت في موقع إلكتروني والمصنفات السينيمائية أيضا، إضافة إلى المصنفات المجسدة في تسجيلات صوتية لهم الحق في التمتع بالحق الإستئثاري في التصريح بتأجير النسخة الأصلية الموضوعة في موقع إلكتروني أو على شبكة الإنترنت أو غيرها من نسخ مصنفاتهم للجمهور لأغراض تجارية ويمثل ذلك التأجير السماح باستخدام نسخة إلكترونية[2].

وينتفي هذا الحق في حالتين:

- إذا تعلق الموضوع ببرنامج حاسوب ،ولم يكن البرنامج في حد ذاته هو موضوع التأجير الأساسي.
- إذا تعلق الموضوع بمصنف سنيمائي ما لم يكن ذلك التأجير قد أدى إلى إنتشار نسخ ذلك المصنف بما يلحق ضررا ماديا بالحق الإستئثاري في الإستنساخ.

---

[1] - راجع نص المادة 6 الفقرة 1و2 من إتفاقية الإنترنت الأولى (الويبو) بشأن حق المؤلف لسنة 1996.

[2] - فاتن حسين حوى- المواقع الإلكترونية وحقوق الملكية الفكرية- دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2010، ص 124.

ويجوز للطرف المتعاقد الذي كان يطبق نظاما قائما على منح المؤلفين مكافأة عادلة مقابل تأجير نسخ عن مصنفاتهم المجسدة في تسجيلات صوتية ،شريطة ألا يلحق تأجير المصنفات المجسدة في تسجيلات صوتية لأغراض تجارية ضررا ماديا بحقوق المؤلفين الإستئثارية في الإستنساخ[1].

1- حق نقل المصنف إلى الجمهور

يتمتع مؤلفو المصنفات الأدبية والفنية بالحق الإستئثاري في التصريح بنقل مصنفاتهم إلى الجمهور بأي طريقة سلكية أو لاسلكية بما في ذلك إتاحة مصنفاتهم للجمهور بما يمكِّن أفراد من الجمهور من الإطلاع على تلك المصنفات من مكان وفي وقت يختارهما الواحد منهم بنفسه ،وذلك دون الإخلال بأحكام المواد ذات الصلة في إتفاقية برن[2].

وقد تبنت الإتفاقية ما يسمى " بالحل الشامل " بالنسبة لما يتعلق بنقل المصنفات عبر الإنترنت ،فبموجبه يتمتع مؤلفو المصنفات الأدبية بالحق في التصريح بنقل مصنفاتهم للجمهور بأية طريقة سلكية أو لاسلكية (بثها وإرسالها عبر البطاقات الرقمية وتداولها على دعامات رقمية) ،مع ترك المشرع الوطني يحدد طبيعته القانونية وحدود المسؤولية الناشئة عنه وعن الإعتداء عليه وفقا للنظام القانوني لكل دولة.

وقد أجازت الإتفاقية في المادة 10 للطرف المتعاقد أن ينص في تشريعه الوطني على تقييدات واستثناءات للحقوق الممنوحة لمؤلفي المصنفات الأدبية والفنية في بعض الحالات الخاصة التي لا تتعارض والإستغلال العادي للمصنف ولا تسبب ضررا بغير مبرر للمصالح المشروعة للمؤلف.

وتطبيقا لهذه المادة فإن استعمال مقتطفات من مصنف منشور في موقع إلكتروني أو على شبكة الإنترنت إستعمالا مشروعا ،كحالات إستعمال المصنف الأدبية والفنية لأغراض التعليم يعد أمرا مسموحا به بشرط أن يذكر إسم المؤلف والمصدر ،ويسمح أيضا بنقل المقالات المنشورة في المواقع الإلكترونية الخاصة بالصحف والدوريات بشروط عامة حددتها إتفاقية **برن** عند الحديث عن التقييدات والإستثناءات[3].

ب- التقييدات التقنية لإدارة حقوق التأليف

[1] - راجع نص المادة 7 الفقرة 1،2،3 من إتفاقية الإنترنت الأولى (الويبو) بشأن حق المؤلف لسنة 1996.

[2] - راجع نص المادة 8 من إتفاقية الإنترنت الأولى (الويبو) بشأن حق المؤلف لسنة 1996.

[3] - فاتن حسين حوى، مرجع سابق، ص 125.

بهدف الوصول إلى حماية قانونية فاعلة لحقوق التأليف وتطبيقها تطبيقا فعالا، وجب اللجوء إلى تدابير تكنولوجية للحماية ومعلومات لإدارة حقوق التأليف، وقد تمّ الإتفاق بين الدول من خلال هذه الإتفاقية على أن يترك تطبيق التدابير والمعلومات لأصحاب الحقوق المعنيين وأن تعتمد أحكام قانونية لحماية أوجه الإنتفاع بتلك التدابير والمعلومات.

وبموجب ذلك ضمّنت الإتفاقية إلتزامات على الأطراف المتعاقدة منها ما هو متعلق بالتدابير التكنولوجية والمعلومات الضرورية لإدارة هذه الحقوق.

1- الإلتزامات المتعلقة بالتدابير التكنولوجية

ألزمت الإتفاقية على الأطراف المتعاقدة أن تنص في قوانينها على حماية مناسبة وجزاءات فعالة ضد التحايل على التدابير التكنولوجية الفعالة التي يستعملها المؤلفون لدى ممارسة حقوقهم بناء على هذه الإتفاقية ،والتي تمنع من مباشرة أعمال لم يصرح بها المؤلفون المعنيون أو لم يسمح بها القانون فيما يتعلق بمصنفاتهم، خاصة منها المتضمَّنة في مواقع إلكترونية[1].

ولاشك أن مثل هذه الأحكام وضعت بغرض مواكبة التطورات التكنولوجية التي ترتكز على الإتصالات وزيادة استخدام أجهزة الكمبيوتر والإنترنت في العديد من التعاملات، وهو ما يفتح المجال لاعتداءات مختلفة وخطيرة على المصنفات الأدبية.

2- الإلتزامات المتعلقة بالمعلومات الضرورية لإدارة الحقوق:

وتلزم الإتفاقية الأطراف المتعاقدة بأن تنص في قوانينها الداخلية على جزاءات مناسبة وفعالة توقع على أي شخص يباشر عن علم أيّاً من الأعمال التالية ، أو لديه أسباب كافية ليعلم – بالنسبة للجزاءات المدنية – أن تلك الأعمال تحمل على إرتكاب تعدٍّ على أي حق من الحقوق التي تشملها هذه المعاهدة أو إتفاقية برن ،او تمكّن من ذلك أو تُسهّل ذلك أو تخفيه[2]، وهذه الأعمال هي:

- أن يحذف أو يغير دون إذن أي معلومات واردة في شكل إلكتروني تكون ضرورية لإدارة الحقوق.

---

[1] - بقنيش عثمان ،مصطفى هنشور وسيمة ،مرجع سابق ،ص 396.

[2] - حسن البدراوي،معايير لحماية دولية في مجال حق المؤلف والحقوق المجاورة، ندوة الويبو الوطنية المتخصصة للسلطات القضائية الأردنية ،القاهرة، 09 أكتوبر 2004 ،ص ص 13-14 ،وثيقة منشورة على الموقع: https://www.wipo.int>mdocs>arab>... تاريخ الإطلاع: 2020/03/28. الساعة: 10:15

- أن يوزع أو يستورد لأغراض التوزيع أو يذيع أو ينقل إلى الجمهور دون إذن مصنفات أو نسخاً على مصنفات ،مع علمه بأنه قد حذفت منها أو غيرت فيها دون إذن معلومات واردة في شكل إلكتروني تكون ضرورية لإدارة الحقوق[1].

يقصد بعبارة " المعلومات الضرورية لإدارة الحقوق " المعلومات التي تسمح بتعريف المصنف ومؤلفه ومالك أي حق فيه ،أو المعلومات التي تتعلق بشروط الإنتفاع بالمصنف وأي أرقام أو شفرات ترمز إلتلك المعلومات متى كان أي عنصر من تلك المعلومات مقترنا بنسخة من المصنف أو ظاهراً لدى نقل المصنف إلى الجمهور، وهو ما أكدته المادة 2/12 من إتفاقية الإنترنت الأولى. ومن خلال هذه الأحكام تتجلى لنا المجهودات التي قامت بها المنظمة العالمية للملكية الفكرية في توفير الحماية لحق المؤلف من الإعتداءات الناجمة عن التطورات التكنولوجية وذلك من خلال أحكام اتفاقية الإنترنت الأولى التي تضمن نطاقا هاما لحماية الملكية الرقمية.

المحور الثاني: القواعد الحمائية للملكية الفكرية في معاهدة الويبو الثانية

برزت هذه الإتفاقية باعتبار أن إتفاقية روما ذات الصلة بالحقوق المجاورة لحق المؤلف لم تعد كافية لمواجهة جميع التطورات والتغيرات التكنولوجية في مجالات تقنيات الفيديو وأنظمة التسجيل المنزلي، بالإضافة إلى البث الفضائي المرئي والمسموع عبر الأقمار الصناعية، بالإضافة لمستجدات البث والتسجيل عبر الإنترنت والدعامات الإلكترونية.

وفي هذا الإطار سنتناول نطاق الحماية المقررة في هذه الإتفاقية، بالإضافة إلى آثار هذه الحماية.

أولا: نطاق الحماية المقررة في ظل إتفاقية الإنترنت الثانية لسنة 1996

نصت المادة 1/1 من إتفاقية الإنترنت الثانية على أنه: " ليس في هذه المعاهدة ما يحد من الإلتزامات المترتبة حاليا على الأطراف المتعاقدة بعضها اتجاه البعض الآخر بناء على الإتفاقية الدولية لحماية فناني الأداء ومنتجي التسجيلات الصوتية وهيئات الإذاعة المبرمة في روما في 26 أكتوبر1961".

وجاءت هذه الإتفاقية لسد النقص المسجل في إتفاقية روما ذات الصلة بالحقوق المجاورة لحق المؤلف[2]، وليس في الإتفاقية ما يحد من الإلتزامات المترتبة حاليا على الأطراف المتعاقدة بناء

---

[1] - راجع نص المادة 12 الفقرة 1 من إتفاقية الإنترنت الأولى (الويبو) بشأن حق المؤلف لسنة 1996.

[2] - إتفاقية روما بشأن حماية فناني الأداء ومنتجي التسجيلات الصوتية وهيئات الإذاعة لسنة 1961.

على إتفاقية روما وليست لهذه الإتفاقية أي صلة بأي إتفاقيات أخرى ،كما لا تخل بأي حقوق او إلتزامات مترتبة عليها[1].

فيما يخص النطاق الموضوعي للحماية فقد أكدت الإتفاقية على أنه تمنح الأطراف المتعاقدة الحماية لفناني الأداء ومنتجي التسجيلات الصوتية من مواطني سائر الأطراف المتعاقدة ،ما وضعوا إنتاجهم على شبكة الإنترنت أو ضمن المواقع الإلكترونية[2].

ومن المبادئ الأساسية التي أكدتها الإتفاقية " مبدأ المعاملة الوطنية "، والذي جاء ذكره في نص المادة 1/4 من إتفاقية الإنترنت الثانية.

كما نصت إتفاقية الإنترنت الثانية في مادتها 1/16 على مجموعة من التقييدات والإستثناءات للحماية الممنوحة في هذه الإتفاقية، فأجازت للطرف المتعاقد أن ينص في تشريعه الوطني على تقييدات واستثناءات للحماية الممنوحة لفناني الأداء ومنتجي التسجيلات الصوتية من النوع ذاته الذي ينص عليه في تشريعه الوطني لحماية حق المؤلف من المصنفات الأدبية والفنية.

وفي ما يخص مدة الحماية الممنوحة لفناني الأداء بموجب هذه الإتفاقية ،فإنها تسري حتى نهاية مدة خمسين سنة على الأقل من نهاية السنة التي فيها تثبيت الأداء في تسجيل صوتي ،أما مدة الحماية الممنوحة لمنتجي التسجيلات الصوتية فتسري حتى نهاية مدة خمسين سنة على الأقل إعتباراً من نهاية السنة التي تم فيها نشر التسجيل الصوتي أو إعتباراً من نهاية السنة التي تم فيها التثبيت إذا لم يتم النشر في غضون خمسين سنة من تثبيت التسجيل الصوتي[3].

ثانيا: أثار الحماية المقررة في إطار إتفاقية الإنترنت الثانية لسنة 1996

نصّت الإتفاقية على العديد من الحقوق والإلتزامات التي تتعلق بالتدابير التكنولوجية والمعلومات الضرورية لإدارة الحقوق المجاورة و الإلتزامات المتعلقة بالمعلومات الضرورية.

أ- حقوق فناني الأداء ومنتجي التسجيلات الصوتية

وتتمثل هذه الحقوق في التالي:

1- حقوق فناني الأداء: وتتفرّع إلى:

---

1 - براهيمي أمين ،مرجع سابق ،ص72.

2 - راجع نص المادة 2 من إتفاقية الإنترنت الثانية (الويبو) بشأن الأداء والتسجيل الصوتي لسنة 1996.

3 - براهيمي أمين ، مرجع سابق، ص73.

- **الحقوق المعنوية:** يحتفظ فنان الأداء فيما يتعلق بأدائه السمعي أو أدائه المثبت في تسجيل صوتي وموضوع على شبكة الإنترنت في موقع إلكتروني بالحق في أن يطالب بأن ينسب أداؤه إليه، وله الحق في الاعتراض على كل تحريف أو تشويه أو أي تعديل آخر لأدائه يكون ضارا بسمعته[1].

كما تبقى حقوقه محفوظة بعد وفاته وإلى حين إنقضاء الحقوق المالية على الأقل ،ويمارس هذه الحقوق الأشخاص أو الهيئات المصرح لها في تشريع الطرف المتعاقد المطلوب توفير الحماية فيه ، ومع ذلك فإن الأطراف التي لا يتضمن تشريعها المعمول به عند التصديق على الإتفاقية أو الإنضمام إليها نصوصا تكفل الحماية بعد وفاة فنان الأداء لكل حقوقه ،ويكون لها الحق في النص على أن بعض هذه الحقوق لا يحتفظ بها بعد وفاته، وفقا لما نصت عليه المادة 1/5 من الإتفاقية[2].

2- حقوق فناني الأداء المالية في أوجه أدائهم غير المثبتة

يتمتع فنانو الأداء بالحق الإستئثاري في التصريح بإذاعة أوجه أدائهم غير المثبة ونقلها إلى الجمهور إلا إذا سبق للأداء أن كان أداء مذاعا، وتثبيت أوجه أدائهم غير المثبة، وهي:

- **حق الإستنساخ**

يتمتع فنانو الأداء بالحق الإستئثاري في التصريح بالإستنساخ المباشر أو غير المباشر لأوجه أدائهم المثبتة في تسجيلات صوتية بأي طريقة أو بأي شكل كان.

- **حق التأجير**

لفناني الأداء الحق الإستئثاري في التصريح بتأجير النسخة الأصلية أو غيرها من النسخ عن أوجه أدائهم المثبتة في تسجيلات صوتية للجمهور لأغراض تجارية حسب التعريف الوارد في القانون الوطني للطرف المتعاقد حتى بعد توزيعها بمعرفة فنان الأداء أو بتصريح منه ،وبالرغم من ذلك إلاّ أنه يجوز للطرف المتعاقد أن يطبق نظاما قائما على منح فناني الأداء مكافأة عادلة مقابل تأجير نسخ عن أوجه أدائهم المثبتة في تسجيلات صوتية ،شرط ألاّ يلحق تأجير

[1] - راجع نص المادة 1/5 من إتفاقية الإنترنت الثانية (الويبو) بشأن الأداء والتسجيل الصوتي لسنة 1996.

[2] - فاتن حسين حوى، مرجع سابق، ص 131.

التسجيلات الصوتية لأغراض تجارية ضرراً مادياً بحقوق فناني الأداء الإستئثارية في الإستنساخ[1].

- **حق التوزيع**

وفقا للمادة 08 يتمتع فنانو الأداء بالحق الإستئثاري في التصريح بإتاحة النسخة الأصلية أو غيرها من النسخ للجمهور ببيعها أو نقل ملكيتها بطريقة أخرى.

- **حق إتاحة الأداء المثبت**

طبقا لأحكام المادة 10 من الإتفاقية، يتمتع فنانو الأداء بالحق الإستئثاري في التصريح بإتاحة أوجه أدائهم المثبتة في تسجيلات صوتية للجمهور بوسائل سلكية أو لاسلكية بما يمكِّن أفراد من الجمهور من الإطلاع عليها من مكان وفي وقت يختارهما الواحد منهم بنفسه[2].

3- حقوق منتجي التسجيلات الصوتية

تشمل هذه الحقوق ذات الحقوق المادية المقررة لفناني الأداء فيتمتع هؤلاء بما يلي:

- **حق الإستنساخ**

وفقا لنص المادة 11 من الإتفاقية، يتمتع منتجو التسجيلات الصوتية بالحق الإستئثاري في التصريح بالإستنساخ المباشر أو غير المباشر لتسجيلاتهم الصوتية بأي طريقة أو بأي شكل.

- **حق التأجير**

أكدت المادة 13 من الإتفاقية، بتمتع منتجو التسجيلات الصوتية بالحق الإستئثاري في التصريح بتأجير النسخة الأصلية وغيرها من نسخ تسجيلاتهم الصوتية للجمهور لأغراض تجارية حتى بعد توزيعها بمعرفة المنتج أو بتصريح منه[3].

- **حق التوزيع**

---

[1] - راجع نص المادة 9 من إتفاقية الإنترنت الثانية (الويبو) بشأن الأداء والتسجيل الصوتي لسنة 1996.

[2] - عبد الله كريم عبد الله، الحماية القانونية لحقوق الملكية الفكرية على شبكة الإنترنت، دار الجامعة الجديدة، القاهرة، 2008، ص 278.

[3] - راجع نص المادة 11،13 من إتفاقية الإنترنت الثانية (الويبو) بشأن الأداء والتسجيل الصوتي لسنة 1996.

يتمتع منتجو التسجيلات الصوتية بالحق الإستئثاري في التصريح بإتاحة النسخة الأصلية أو غيرها من نسخ تسجيلاتهم الصوتية للجمهور ببيعها أو نقل ملكيتها بطريقة أخرى.

- **حق إتاحة التسجيلات الصوتية**

تخول المادة 14 من الإتفاقية لمنتجي التسجيلات الصوتية بالحق الإستئثاري في التصريح بإتاحة تسجيلاتهم الصوتية للجمهور بوسائل سلكية أو لاسلكية بما يمكّن أفرادا من الجمهور من الإطلاع عليها من مكان وفي وقت يختارهما الواحد منهم بنفسه.

ويتضح لنا مما ذكرناه أن هناك إختلاف بين القواعد المتعلقة بفناني الأداء من جهة وحقوق منتجي التسجيلات الصوتية من جهة ثانية ،والمتمثل في النص على الحقوق المادية والمعنوية دون أن يكون هناك نص مماثل بالنسبة لحقوق منتجي التسجيلات الصوتي.

ب- الإلتزامات المتعلقة بالتدابير التكنولوجية والمعلومات الضرورية لإدارة الحقوق المجاورة

يمكن تلخيص هذه الإلتزامات على النحو التالي:

1- الإلتزامات المتعلقة بالتدابير التكنولوجية لإدارة الحقوق

طبقا لأحكام المادة 18 من الإتفاقية، فإنه يتوجب على الأطراف المتعاقدة أن تنص في قوانينها على حماية مناسبة وعلى جزاءات فعالة ضد التحايل على التدابير التكنولوجية والفعالة التي يستغلها فنانو الأداء أو منتجو التسجيلات الصوتية بالإرتباط بممارسة حقوقهم بناء على هذه الإتفاقية ،والتي تمنع من مباشرة أعمال لم يصرح بها أو يسمح بها القانون فيما يتعلق بأوجه أدائهم أو تسجيلاتهم الصوتية، ويعني ذلك إلزام الدولة بإصدار قوانين أو تشريعات تتضمن قواعد توفر الحماية المناسبة لها وجزاءات انتهاك التدابير التكنولوجية الفعالة وإجراءات الحماية التقنية التي يستعملها فنانو الأداء ومنتجو التسجيلات الصوتية لحماية حقوقهم من التعدّي، وينصرف ذلك إلى وجود هذه الأعمال على شبكة الإنترنت وفي المواقع الإلكترونية، وتضمن هذه المواقع حماية تقنية يعاقب من يحاول خرقها[1].

2- التدابير المتعلقة بالمعلومات الضرورية لإدارة الحقوق المجاورة

[1] - فاتن حسين حوى، مرجع سابق، ص 135.

ألزمت الإتفاقية الأطراف المتعاقدة على أن تنص في قوانينها على توقيع جزاءات مناسبة وفعالة توقع على أي شخص يباشر عن علم أياً من الأعمال التالية وهو يعرف أو كان بإمكانه أن يعرف أن تلك الأعمال تؤدي إلى إرتكاب تعدٍّ على أي حق من الحقوق التي تشملها هذه الإتفاقية أو تُمكِّن من ذلك أو تسهل ذلك أو تخفيه، وهذه الأعمال هي:

- أن يحذف أو يغير دون إذن أي معلومات واردة في شكل إلكتروني تكون ضرورية لإدارة الحقوق.
- أن يوزع أو يستورد لأغراض التوزيع أو يذيع أو ينقل إلى الجمهور أو يتيح له دون إذن أوجه أداء مثبتة أو تسجيلات صوتية مع علمه بأنه قد حذفت منها أو غيرت فيها ودون إذن معلومات واردة في شكل إلكتروني تكون ضرورية لأداء الحقوق[1].
- كما تتطلب الإتفاقية من الدول الأطراف اتخاذ التدابير اللازمة لضمان تطبيق أحكامها، كما تكفل للأطراف المتعاقدة أن تتضمن قوانينها إجراءات إنفاذ تسمح باتخاذ تدابير فعالة ضد أي تعدّ على الحقوق التي تغطيها هذه الإتفاقية، بما في ذلك توقيع الجزاءات العاجلة لمنع التعديات الأخرى[2]، وفقا لما نصت عليه المادة 2/23 من الإتفاقية.
- **خاتمة:**

إن موضوع الحماية الدولية للملكية الفكرية اكتسى أهمية بالغة، حيث سعى المشرع الدولي جاهدا إلى تجسيد هذه الحماية وترجمتها واقعيا، فتظافرت الجهود الدولية لإيجاد تنظيم قانوني شامل أو مايسمى بـ " القانون الدولي للملكية الفكرية " يكفل حماية هذه الحقوق ويتأقلم مع مختلف التطورات التي يعرفها العالم، ولأجل ذلك تم إبرام العديد من الاتفاقيات الدولية أبرزها إتفاقيتي الإنترنت الأولى والثانية، والتي تبنتها المنظمة العالمية للملكية الفكرية.

وفي هذا الإطار ومن خلال الطراح السالف للذكر، حاولنا صياغة بعض الإقتراحات نذكرها كالتالي:

---

[1] - راجع نص المادة 19 من إتفاقية الإنترنت الثانية (الويبو) بشأن الأداء والتسجيل الصوتي لسنة 1996.

[2] - المكتب الدولي، تأثير التكنولوجيا الجديدة في حماية حقوق الملكية الفكرية، ص 07، مقال متوفر على الموقع: www.arabpipr.org تاريخ الإطلاع: 2020/03/30. الساعة: 18:20.

- على المشرع الدولي العمل على تفعيل نصوص هذه الإتفاقيات من خلال وضع آليات تشرف على تنفيذها وتساعد الدول على إعمالها ومواءمتها ضمن تشريعاتها الداخلية.
- تنظيم جوانب الملكية الفكرية المرتبطة ببرامج الحاسب والإنترنت.
- ضرورة التنسيق بين المنظمات الدولية والإقليمية المعنية بحقوق الملكية الفكرية ، والتعاون الدولي في مكافحة الجريمة المعلوماتية.
- العمل على توسيع مضمون الإتفاقيات الحديثة نظرا للتطور التكنولوجي الكبير، والتحول من عالم الأوراق إلى العالم الإفتراضي.
- إنشاء أجهزة وهيئات لمتابعة مدى تنفيذ هذه الإتفاقيات مع مراعاتها جانب الدول النامية دائما.
- العمل على إنشاء محاكم دولية خاصة بالملكية الفكرية، وتكوين قضاة متخصصين في هذا المجال.

الاتفاقيات الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية

International and regional agreements in the field of combating electronic crime

د.عطار نسيمة استاذة محاضرة ب
معهد الحقوق و العلوم السياسية
المركز الجامعي مغنية - الجزائر

مقدمة

لقد شهد العالم تطورا في شتى مجالات الحياة، وقد ترجم هذا التطور في ظهور مفاهيم جديدة من بينها الشبكة العنكبوتية التي أصبحت العصب الرئيسي للثورة المعلوماتية، حيث أضحى العالم قرية صغيرة سهلة الوصول والاتصال.

وحقيقة لا يمكن إنكارها أن من أهم انجازات العلم في العصر الحديث، وأعظمها جدوى للإنسان، هي ظهور الحاسب الآلي والأنترنت، الذين قدما خدماتهما للإنسانية، في أغلب مناحي الحياة الاقتصادية والتعليمية والطبية والعديد من المجالات الأخرى.

لكن هذا التطور الذي عرفته البشرية في المجال المعلوماتي، وبالموازاة مع طبيعة السلوك البشري، الذي رافقته الجريمة منذ القدم لم يجعل هذا التطور التكنولوجي مقتصرا على النفع والسلوك السوي، بل اتخذ من وسائل الاتصال الالكترونية أرضا خصبة لارتكاب سلوكات إجرامية بات يطلق عليها الجريمة الالكترونية. حيث استغل اصحاب وذوي الخبرة الفنية والتقنية في هذا المجال خبرتهم، للقيام بأعمال اجرامية أدت إلى ظهور مفهوم جديد للجريمة التقليدية، التي حولت هذه الأخيرة من صفتها العادية وأبعادها المحدودة إلى أبعاد جديدة تعتمد على التقنية والخبرة الفنية في ارتكابها.

فالجريمة المعلوماتية تعتبر من بين الظواهر الحديثة، نتيجة ارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات. وماتجدر الاشارة إليه هو الغموض واللبس الذي أحاط بمفهوم الجريمة المعلوماتية، والذي دفع بالفقه والقانون إلى بذل مجهود في توحيد التعريفات التي قيلت في صدد تعريفها.

وإن موضوع الجريمة المعلوماتية يعرف أهمية متزايدة بالنظر للاستغلال مرتكبي الجرائم الالكترونية للوسائل الحديثة للاتصال لأجل تسهيل عملية ارتكاب جرائمهم وتنامي أعداها بصورة مهولة، وإن هذا الموضوع يكتسي أهمية من ناحيتين أساسيتين هما:

-أن الجريمة المعلوماتية أثر بالغ في مجمل مصالح المجتمع، وانتهاكها للقواعد القانونية التي تحمي الفرد والمجتمع.

-أن الجريمة المعلوماتية شكلت دافع لتعاون الجهود الدولية و الإقليمية في مكافحتها.

وبالنظر إلى الدور الفعال المبذول على المستوى الدولي وكذلك على المستوى الإقليمي، لنا أن نتساءل عن مضمون هذه المجهودات المبذولة علي مستوى الصعيدين في مكافحة الجريمة المعلوماتية؟

للإجابة على هذه الإشكالية سيتم الاعتماد على المنهج الوصفي في تحديد هذه الجريمة والوقوف على تقسيماتها، إضافة إلى المنهج التحليلي لأهم الصكوك الدولية والإقليمية التي جاءت مكافحة لها.

وبناء على ما سبق سيتم تقسيم خطة البحث إلى عنوانين رئيسين هما:

المبحث الأول: مفهوم الجريمة المعلوماتية

المبحث الثاني: الصكوك الدولية و الاقليمية في مكافحة الجريمة المعلوماتية.

المبحث الأول: مفهوم الجريمة المعلوماتية

يمكن الجزم بأن الجريمة الالكترونية لا تعرف تعريف جامع وشامل لها، حيث تعددت الآراء والتعريفات بشأنها، وذلك نتيجة الاختلاف في وجهة النظر الفقهية التي تناولها (كمطلب أول)، وتقسيماتها (كمطلب ثان)

المطلب الأول: تعريف الجريمة المعلوماتية:

لقد اختلفت الآراء بشأن تعريف الجريمة الالكترونية، فهناك من عرفها انطلاقا من زاوية فنية، وهناك من عرفها من زاوية قانونية، وهناك من عرفها بالنظر إلى وسيلة ارتكابها أو موضوعها، أو حسب توافر المعرفة بتقنية المعلومات لدى مرتكبها أو استنادا لمعايير أخرى حسب القائلين بها[1].

[1] - عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار مدبولي، القاهرة 2009، ص. 115.

فالجريمة المعلوماتية تعرف على أنها كل عمل أو امتناع يأتيه الانسان ويحدث أضرارا بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به. كا عرفت بأنها نشاطا إجراميا تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة وسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود.

كما عرفت أيضا بانها نشاط جنائي يمثل اعتداء على برامج وبيانات الحاسب الالكتروني. كما عرفت بأنها كل استخدام في صورة فعل أو امتناع غير مشروع للتقنية المعلوماتية، ويهدف إلى الاعتداء على أي مصلحة مشروعة، سواء أكانت مادية أو معنوية[1].

وإنه رغم الفارق بين ميدان جرائم الحاسب الآلي، وميدان جرائم الانترنت، فبينما تحقق الأولى من خلال الاعتداء على مجموعة الأدوات المكونة للحاسب وبرامجه والمعلومات المخزنة به، فإن جرائم الانترنت تحقق بنقل المعلومات والبيانات بين أجهزة الحاسب عبر خطوط الهاتف أو الشبكات الفضائية، إلا أن الواقع التقني أدى إلى اندماج الميدانين (الحوسبة والاتصالات)[2].

من خلال التعريفات السابقة نميز الخلاف والاختلاف في مضمون التعربفات السابقة، ويمكن إبراز هذا الاختلاف اعتمادا على المعيار والأساس الذي تم وضعه لأجل تحديد تعريف هذا النوع من الجرائم، والذي نجمله في النقاط التالية:

الفرع الأول: تعريفات تستند إلى موضوع الجريمة ووسيلة ارتكابها:

أولا: تعريفات تستند إلى موضوع الجريمة

عرفها أنصاره بأنها كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات، حيث يرى أنصار هذا الاتجاه أن الجريمة الالكترونية، ليست هي التي يكون النظام المعلوماتي أداة ارتكابها، بل هي التي تقع عليه أو في نطاقه.

وهنا من عرفها بأنها نشاط غير مشروع موجه، لنسخ أو تغيير أو حذف أو الوصول، إلى المعلومات المخزنة داخل الحاسب، أو التي تحول عن طريقه[3].

ثانيا: تعريفات تستند إلى وسيلة ارتكابها:

1 - سعيداني سلامة، المرجع السابق، ص. 193.

2 - محمد السعيد زناتي، المرجع السابق، ص. 30.

3 - أحمد خليفة الملط، الجرائم المعلوماتية، طبعة الأولى، دار الفكر الجامعي، الاسكندرية، 2006، ص. 85.

فهي الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا، في ارتكابها. ووفقا لهذا الاتجاه فإن التركيز في التعريف ينصب على الوسيلة التي ترتكب بموجبها الجريمة، وتمثل هنا باستخدام الحاسوب.

الفرع الثاني: تعريفات تستند إلى شخص الفاعل:

عرفها أنصار هذا الاتجاه بأن الجريمة الالكترونية هي الجريمة التي يثبت لمرتكبها، معرفة فنية بالحسابات تمكنه من ارتكابها. كما عرفت بأنها أي فعل غير مشروع تكون المعرفة بتقنية الحاسوب أساسية، لارتكابه والتحقيق فيه وملاحقته قضائيا.

فهذه التعريفات كلها تنطلق من معيار شخصي، يتمثل في وجوب توفر المعرفة التقنية لمرتكبها، حيث تنصب على سمة الفاعل.

الفرع الثالث: التعريف الأقرب للصواب والشمولية:

يعد التعريف المعتمد من قبل مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين، الأقرب للصواب، حيث عرف الجريمة الالكترونية، بأنها أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية.

حيث يمتاز هذا التعريف بأنه حاول الإحاطة بجميع الأشكال الإجرامية للجريمة الالكترونية، سواء أكانت التي تقع بواسطة النظام المعلوماتي، أم داخل هذا النظام على المعطيات والبرامج والمعلومات، كما شمل التعريف جميع الجرائم التي من الممكن أن تقع في بيئة إلكترونية[1].

المطلب الثاني: تقسيمات الجرائم الالكترونية:

الفرع الأول: جرائم الحاسب الآلي:

يقصد بها مجموع الأفعال التي تشكل اعتداء على أجهزة الحاسب الآلي، سواء على مكوناته المادية مثل وحدات الإدخال والإخراج، ووسائل التخزين المرنة والصلبة أو الشاشة والطابعة. أو على مستوى مكوناته المعنوية كالبيانات والمعلومات المخزنة داخل الحاسب الآلي، وعلى ذلك فإن جرائم الحاسب تختلف حسب طبيعة الشيء محل الاعتداء، ذلك أن الاعتداء أحيانا يقع على أدوات وآلات الحاسب الآلي، وأحيانا أخرى يقع على برامج ومعلومات داخل الحاسب الآلي.

---

[1] - أحمد أسامة حسنية، الجريمة الالكترونية بين الشرعية الجنائية والإجرائية، مجلة جامعة الأزهر، عدد خاص بمؤتمر كلية الحقوق الخامس المحكم، المجلد 19، 2017، ص.7.

الفرع الثاني جرائم الانترنت:

وهي كل فعل غير مشروع يقع على مواقع الانترنت، بقصد تعطيلها أو تشويهها أو تعديلها، والدخول غير المشروع لمواقع غير مصرح بالدخول إليها، واستخدام عناوين غير حقيقية للدخول في شبكة المعلومات واقتحام الشبكات ونقل الفيروسات، وإرسال الرسائل بكافة أنواعها عبر البريد الالكتروني، كالماسة بكرامة الأشخاص أو المستهدفة ترويج مواد أو أفعال غير مشروعة[1].

الفرع الثالث: جرائم شبكة المعلومات:

يمكن تصور عدة طرق للتلاعب بالنظام المعلوماتي، فقد يكون التلاعب في المعلومات الموجودة على النظام المعلوماتي، بطريقة مباشرة عن طريق إدخال معلومات غير موجودة ولا أساس لها من الصحة، أو إتلاف المعلومات في مجال المعلوماتية بالاعتداء على الوظائف الطبيعية للحاسب الآلي، وذلك بالتعدي على البرامج والبيانات المخزنة والمتبادلة بين الحواسب وشبكاته، وتدخل ضمن الجرائم الماسة بسلامة المعطيات المخزنة ضمن النظام المعلوماتي، ويكون الإتلاف العمدي للبرامج والبيانات كمحوها أو تدميرها الكترونيا، أو تشويهها على نحو يجعلها غير صالحة للاستعمال[2].

المبحث الثاني: الصكوك الدولية و الإقليمية في مكافحة الجريمة المعلوماتية.

لقد تنوعت الاتفاقيات على نوعيها في تحديد الجريمة المعلوماتية، وتحديد سبل مكافحتها، وفي هذا الشق من الدراسة سنصب الاهتمام على مجموعة من الاتفاقيات الدولية والإقليمية التي قيل بها في هذا الصدد.

المطلب الأول: الاتفاقيات الدولية في مجال مكافحة الجريمة المعلوماتية:

سنحاول في هذا الجزء من البحث إلى التعرض لأهم الاتفاقيات الدولية التي جاءت مكافحة للجريمة المعلوماتية.

الفرع الأول: اتفاقية برن:

---

[1] - المرجع نفسه، ص. 30.

[2] - سورية ديش، أنواع الجرائم الالكترونية وإجراءات مكافحتها، مجلة العلوم السياسية والقانون، عدد 1، المركز الديمقراطي العربي، فبراير 2017، ص. 145.

تعد اتفاقية برن التي تم التوقيع عليها في عام 1971 في سويسرا[1]، حجر الأساس في مجال الحماية الدولية لحق المؤلف، وقد وقعت على هذه الاتفاقية 120 دولة، وتعد المادة التاسعة من هذه الاتفاقية هي الأساس لأنها تنص على منح أصحاب حقوق المؤلف حق استئثاري، في التصريح بعمل نسخ من هذه المصنفات بأي طريقة وبأي شكل كان[2].

وقد عرفت هذه الاتفاقية عدة تعديلات، حيث جاءت اتفاقية باريس مكملة لها في ماي 1896، والمعدلة في برلين في 13 سبتمبر 1908، والمكملة ببرن في مارس 20 مارس 1914، والمعدلة بروما في جوان 1928، وبروكسل سنة 1948، واستوكهولم في جويلية 1967، وباريس في جويلية 1971، حيث تشكل الدول الأطراف في هذه الاتفاقية اتحادا لحماية حقوق المؤلفين على مصنفاتهم الأدبية والفنية[3].

وفضلا عن ذلك تمنح اتفاقية برن صاحب الحق المؤلف الحق، في أن يرخص أو يمنع أي ترجمة أو اقتباس أو بث إذاعي أو توصيل إلى الجمهور لمصنفه، وكذا تلزم الاتفاقية بتوقيع جزاءات سواء أكان المؤلف المعتدى عليه وطنيا أو أجنبيا[4].

ويرجع الاهتمام بحق المؤلف إلى أنه الوسيلة القانونية الرئيسية لحماية حقوق المؤلفين، فحق المؤلف من أهم الحقوق التي تكفلها النظم القانونية على اختلافها للمبدعين والمؤلفين حماية لإبداعاتهم الفكرية، وإن لم يكن أهمها على الإطلاق، ويوفر هذا الحق -بشروط معينة- لمؤلفي مصنفات معينة في الآداب والفنون والعلوم، أيا كان نوع هذه المصنفات، أو أهميتها، أو طريقة

---

[1] - المرسوم الرئاسي رقم 79-341 المؤرخ في 13-09-1997 المتضمن انضمام الجزائر مع التحفظ إلى اتفاقية برن المؤرخة في 09-09-1869، والمتممة في باريس 04-05-1909، والمعدلة في 28-09-1997، ج ر ج ج، عدد 01، المؤرخة في 14-09-1997.

[2] - بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة دكتوراه في القانون العام، كلية الحقوق، جامعة الجزائر 01، 2018، ص. 14.

[3] - محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة إيليزا للبحوث والدراسات، العدد 2، المركز الجامعي إيليزي، الجزائر، ديسمبر 2017، ص. 36.

[4] - منير محمد الجنبيهي وممدوح محمد الجنبيهي، جرائم الانترنت والحساب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية، 2005، ص. 201.

التعبير عنها أو الغرض من تصنيفها حماية قانونية لا بأس بها لمدة زمنية معينة[1]. وقد تم التأكيد على هذا النوع من الحماية كذلك في اتفاقية الجات التي تفرعت عنها عدة اتفاقيات من بينها اتفاقية حماية حقوق الملكية الفكرية.

وإن اتفاقية برن كأي اتفاقية دولية تقوم على مجموعة من المبادئ الأساسية، التي تحدد نطاق الحماية والواجبة وأسلوب تطبيقها، هذه المبادئ لا تتغير مع التعديلات أو البروتوكولات التي قد يتم إدخالها على الاتفاقية، ويتم حصرها في مبدأين هامين هما:

مبدأ المعاملة الوطنية الذي يقصد به تمتع جميع المصنفات الخاضعة لحماية الاتفاقية في إقليم أي دولة عضو في الاتفاقية، بنفس الحماية التي تمتع بها المصنفات الوطنية لهذه الأخيرة لدى لدولة أخرى طرف في اتفاقية برن.

كما نجد كذلك مبدأ الحد الأدنى من الحماية الذي حاول من خلاله واضعو اتفاقية برن توحيد مستوى الحماية التي تتمتع بها المصنفات، من خلال وضع حد أدنى للحماية لها، لأجل ضمان ألا يقل مستوى الحماية في أي دولة متعاقدة، وذلك لأجل مواجهة التفاوت التشريعي بين مستويات الحماية في الأنظمة القانونية المختلفة[2].

الفرع الثاني: اتفاقية تريبس:

لقد حظيت حقوق الملكية الفكرية بحماية خاصة، على المستوى الدولي نظرا للكم الهائل من الاتفاقيات والمعاهدات المبرمة بشأنها، ولقد ازداد مجال الاهتمام دوليا بهذه الحقوق خاصة بعد انشاء منظمة التجارة العالمية، في 15 أفريل 1994، ووجود اتفاقية سميت باتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية، والمعروفة اختصارا باتفاقية تريبس.

وهي تمثل بلا شك من أهم الاتفاقيات الدولية على الإطلاق، نظرا لما استحدثته من أحكام موضوعية جاءت مغايرة ومختلفة عما جاءت به باقي الاتفاقيات الدولية، التي سبقتها في هذا الموضوع، خاصة ما يتعلق بموضوع الملكية الفكرية[3].

---

[1] - سعيداني سلامي، تطور التشريعات والاتفاقيات الدولية في مجال الجرائم المعلوماتية (وقائع ومقاربات)، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، العدد 10، المجلد 01، جامعة محمد بوضياف، المسيلة، الجزائر، جوان 2018، ص. 201.

[2] - رشا علي الدين، النظام القانوني لحماية البرمجيات، دار الجامعة الجديدة، الاسكندرية، 2007، ص. 241.

[3] - عامر محمود الكسواني، الملكية الفكرية، الطبعة الأولى، دار وائل للنشر، الأردن، 2011، ص. 14.

وجاءت متكونة الاتفاقية من دباجة وثلاث وسبعين مادة، جاءت موزعة على سبعة أجزاء، وقد جاءت بأحكام تفصيلية هدفها الأساسي هو تحرير التجارة العالمية[1].

وإن أهم ما تضمنته اتفاقية تريبس هي مجموع الإجراءات الهامة والفعالة، لردع الاعتداءات على حقوق الملكية الفكرية[2]، كما أنها ومن جهة أخرى تفرض على الدول اتخاذ العديد من التدابير الهامة لمعالجة الوضع، ومن تلك التدابير على سبيل المثال لا الحصر، إعطاء الحق للسلطات في إصدار الأوامر، بشن حملات مفاجئة لضبط أدلة ارتكاب الجريمة، والتي عادة ما تكون سهلة التخلص منها، لو لم تكن هناك سرعة في محاولة ضبطها وذلك التحفظ على أدوات ارتكاب الجرائم، وذلك فضلا عن فرض عقوبات جنائية رادعة[3].

ولفعالية هذه الإجراءات اشترطت الاتفاقية على الدول الأعضاء لحماية حقوق الملكية، المنصوص عليها في هذه الاتفاقية، وبهدف تسهيل اتخاذ تدابير فعالة ضد أي تعدي على حقوق الملكية الفكرية، التي تناولتها الاتفاقية، يجب اتخاذ إجراءات سريعة لمنع التعديات والانتهاكات الحالة في المادة 41 من الاتفاقية.

وضرورة توافر إجراءات قضائية ومدنية إلى جانب إجراءات إدارية أخرى منصوص عليها في المادة 41 من الاتفاقية.

هذا ونصت المادة التاسعة من الاتفاقية على أنه على الدول الأعضاء، فيها الالتزام بأحكام المواد من 01 إلى 21 من معاهدة برن لسنة 1971، مع مراعاة أن الحماية تسري على المنتوج وليس فقط الأفكار، كما نصت على الحماية الزمنية لهذه المصنفات وحددتها بمدى حياة المؤلف بالإضافة إلى مدة خمسين عاما بعد وفاته[4].

وقد أخذت اتفاقية تريبس بنفس المبادئ التي قامت عليها اتفاقية برن لسنة 1971، وهما مبدأ المعاملة الوطنية ومبدأ الحد الأدنى من الحماية، مع إضافة مبدأين هما مبدأ الدولة الأولى بالرعاية، الذي مفاده أن كل دولة عضو في الاتفاقية، إذا ما قامت بمنح أي ميزة تفضيلية معينة، يتعين عليها منح جميع الدول الأعضاء الأخرى نفس الميزة .

---

[1] - عبد الرحيم عنتر عبر الرحمان، حقوق الملكية الفكرية وأثرها الاقتصادي، الطبعة الأولى، دار الفكر الجامعي، مصر، 2007، ص. 120.

[2] - حواس فتيحة، حماية المصنفات الرقمية وأسماء النطاقات على شبكة الانترنت، أطروحة دكتوراه، جامعة الجزائر 01، 2016، ص. 127.

[3] - سعيداني سلامة، المرجع السابق، ص. 201

[4] - بدري فيصل، المرجع السابق، ص. 22.

ومبدأ المعاملة التفضيلية للدول النامية، وهذا مراعاة لظروف هذه الأخيرة، حيث تراعي المرونة في تنفيذ أحكامها على الصعيد الداخلي للدول النامية الأعضاء في اتفاقية تريبس، فاتفاقية تريبس أرادت من المعاملة التفضيلية للدول النامية، تمكين هذه الدول من انشاء قاعدة تكنولوجية متطورة، تخدم مصالحها الاقتصادية وتساعدها في اللحاق بعجلة التجارة الدولية.

الفرع الثالث: معاهدة الويبو:

تم التوقيع على اتفاقية الويبو المنشئة للمنظمة العالمية للملكية الفكرية (الويبو)، في استوكهولم في 14جولية 1967 ودخلت حيز التنفيذ سنة 1970 وعدلت سنة 1979، والويبو عبارة عن منظمة دولية حكومية أصبحت في عداد الوكالات المتخصصة التابعة لمنظومة الأمم المتحدة سنة 1974.

ويرتقي تاريخ إنشاء الويبو إلى سنتي 1883 و1886 عندما أبرمت اتفاقية باريس لحماية الملكية الصناعية واتفاقية برن لحماية المصنفات الأدبية والفنية على التوالي. وقد نصت كلتا الاتفاقيتين على إنشاء "مكتب دولي" وتم توحيد المكتبين الدوليين 1893 وحلت المنظمة الدولية للملكية الفكرية، مكانهما بناء على اتفاقية الويبو سنة 1970 بموجب اتفاقية الويبو.

وقد بلغ عدد الدول الأعضاء في هذه المنظمة عام 1999 إلى 177 دولة، وترتكز نشاطات واختصاصات هذه المنظمة، في دعم حماية للملكية الفكرية بفرعيها، الملكية الأدبية في جميع أنحاء العالم بفضل تعاون الدول مع بعضها البعض في هذا المجال[1]، وقد انقسمت معاهدة الويبو إلى ثلاث معاهدات هي كالآتي:

معاهدة الويبو بشأن حق المؤلف، ومعاهدة الويبو بشأن الأداء والتسجيل الصوتي، ومعاهدة الويبو بشأن الحماية الدولية لحق المؤلف والحقوق المجاورة، تم التوقيع عليهم في 20 ديسمبر1996[2].

الفرع الثالث: قانون الأونيسترال النموذجي:

ينقسم هذا القانون إلى قانون الأونيسترال النموذجي المتعلق بالتجارة الالكترونية، والقانون النموذجي المتعلق بالتوقيعات الالكترونية، وتم صياغة هاذين القانونين اقتناعا من الدول بضرورة مكافحة هذا النوع من الجرائم.

أ) قانون الأونيسترال النموذجي المتعلق بالتجارة الالكترونية:

---

[1] - محمود عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، 2009، ص. 160.

[2] - بدري فيصل، المرجع السابق، ص. 21.

تنطبق نصوص هذا القانون على أي نوع من المعلومات، التي تكون في شكل رسالة بيانات مستخدمة في سياق أنشطة تجارية، بحيث يتم استلامها أو تخزينها بوسائل الكترونية، ويتم تبادل هذه البيانات من خلال نقلها الكترونيا من حاسوب إلى آخر باستخدام معيار متفق عليه، مع الأخذ بعين الاعتبار تفسير هذا القانون لمصدره الدولي ولضرورة توحيد تطبيقه.

ب) قانون الاونيسترال النموذجي المتعلق بالتوقيعات الالكترونية:

اعتمد هذا القانون في 05 جويلية 2001 وينطبق هذا القانون حيثما تستخدم توقيعات الالكترونية، خاصة بعدما أصبح التوقيع بمفهومه التقليدي لا يستجيب لمتطلبات السرعة والحداثة التكنولوجية، حيث أنه أمام هذه التطورات تلاشت وظيفة التوقيع التقليدي، ليحل محله التوقيع الالكتروني، وهو عبارة عن كود سري أو شفرة سرية يتم الحصول عليها بعد إتباع جملة من الاجراءات[1].

المطلب الثاني: الجهود الاقليمية في مكافحة الجريمة المعلوماتية:

تجلى الجهود الإقليمية في مكافحة الجريمة المعلوماتية، في مجموع المساعي التي بذلها المجلس الأوروبي، الذي برز دوره كعنصر فعال في مكافحة هذه الجريمة، لما فيه من ضمان في المحافظة على المعطيات الفردية، وكل ما يتعلق بالحياة الخاصة، ويرجع السبب في ذلك في أن جميع الدول المنضمة إلى المجلس الأوروبي هي دول متطورة علميا وتقنيا، الأمر الذي دفعها في بذل جهد في مجال مكافحة الجريمة المعلوماتية[2].

بالإضافة إلى الجهود التي تبذلها جامعة الدول العربية، من خلال اعتمادها عبر أمانة مجلس وزراء العدل العرب، لما سمي بقانون الإمارات العربي الاسترشادي، لمكافحة جرائم تقنية المعلومات وما في حكمها، نسبة إلى مقدم هذا المقترح، الممثل في دولة الإمارات العربية المتحدة[3].

الفرع الأول: معاهدة بودابست لمكافحة جرائم المعلوماتية والاتصالات:

---

[1] - شريف محمد الغنام، حماية العلامات التجارية عبر الانترنت في علاقتها بالعنوان الالكتروني، دار الجامعة الجديدة، الاسكندرية، 2007، ص. 194.

[2] - سعيداني نعيم، آاليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، جامعة باتنة، 2013، ص. 44.

[3] - بدري فيصل، المرجع السابق، ص. 27.

شهدت العاصمة المجرية بودابست في أواخر عام 2001 ميلاد أولى المعاهدات الدولية التي تكافح جرائم الانترنت، وتبلور التعاون والتضامن الدولي في محاربتها، ومحاولة الحد منها خاصة بعد أن وصلت تلك الجرائم إلى حد خطير أصبح يهدد الأشخاص والممتلكات[1].

ولقد تم صياغة هذه المعاهدة من جانب عدد كبير من الخبراء القانونيين، في مجلس أوروبا، وبمساعدة دول أخرى لاسيما الولايات المتحدة الأمريكية، وبعد مشاورات عديدة بين الحكومات، وأجهزة الشرطة وقطاع الكمبيوتر على مستوى العالم، وهو الأمر الذي أدى في النهاية إلى التوقيع عليها من قبل ثلاثين دولة بتاريخ 23 نوفمبر 2001 في العاصمة المجرية بودابست، وذلك لمواجهة الاستخدام غير المشروع للحسابات، وشبكات المعلومات فيما يعرف بالإجرام الالكتروني أو الإجرام المعلوماتي أو الجرائم المعلوماتية[2].

حيث تم التوقيع عليها من طرف ثلاثون دولة في العاصمة المجرية "بودابست" نذكر منها دول الأعضاء في الاتحاد الأوروبي، كندا، اليابان، جنوب إفريقيا، أمريكا، وجاءت هذه الاتفاقية لتعالج إشكالية دولية الجريمة الالكترونية، وتجاوزها للحدود الدولية، بما يساعد الدول على مكافحة هذه الجريمة وتعقب مرتكبيها، والمساعدة على الاستدلال عليهم وضبطهم، كما تحدد أفضل الطرق الواجب إتباعها في التحقيق، في جرائم الانترنت التي تعهد الدول الموقعة بالتعاون الوثيق، من أجل مكافحتها[3].

وقد اشتملت الاتفاقية الأوروبية لجرائم الحاسب الآلي والانترنت المسماة باتفاقية بودابست الموقعة في 23-11-2001 على خمسة عناوين هي كالآتي:

1) الجرائم التي تمس سرية وأمن وسلامة وتوفير بيانات الحاسب، ومنظوماته وهي تضم (الدخول غير المشروع، والإعراض غير المشروع، والتدخل في البيانات ،والتدخل غير المشروع في المنظومة، وإساءة استخدام الأجهزة).

2) الجرائم المتصلة بالحاسب الآلي، وتضم (جريمة التزوير المتعلقة بالحاسب، وجريمة التدليس المتعلقة بالحاسب)

3) الجرائم المتصلة بالمواد الإباحية للأطفال (الإنتاج أو النشر غير المشروع للمواد الإباحية، وصور الأطفال الفاضحة).

---

[1] - منير محمد الجنبيهي وممدوح محمد الجنبيهي، المرجع السابق، ص. 96.

[2] - محمد علي العريان، الجرائم المعلوماتية، دار الجاعة الجديدة، الاسكندرية، 2011، ص. 25.

[3] - محمد السعيد زناتي، المرجع السابق، ص. 37.

4) الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المرتبطة بها (طبع والنشر).

5) أما العنوان الأخير فخصص للمسؤولية وللجزاءات، وهو يشتمل على بنود إضافية بشأن الشروع والاشتراك، وأيضا الجزاءات أو التدابير، وذلك طبقا للاتفاقيات أو المعايير الدولية الحديثة بالنسبة لمسؤولية الأشخاص المعنوية[1].

ولقد ركزت اتفاقية بودابست على ثلاثة عناصر أساسية:

العنصر الأول: يتمثل في أهمية التدابير التشريعية الموضوعية أي نصوص التجريم الموضوعية.

العنصر الثاني: يتمثل في أهمية التدابير التشريعية الإجرائية المتلائمة مع طبيعة الجرائم الالكترونية أي النصوص الإجرائية.

العنصر الثالث: يتمثل في أهمية تدابير التعاون الدولي والإقليمي، في مجال مكافحة الجرائم[2].

ولقد قام واضعو الاتفاقية بتحديد الإطار العام لهذه الجرائم، والمتمثل في الدخول غير المشروع أو الاعتراض غير المشروع أو الاعتداء على سلامة البيانات أو النظام المعلوماتي، وكذلك إساءة استخدام أجهزة الحسابات أو التزوير المعلوماتي أو الغش المعلوماتي، وقد أوجبت اتفاقية بودابست بعض الشروط حتى تأخذ الأفعال المنصوص عليها فيها وصف الجريمة[3]، نسردها كالآتي:

- أن ترتكب الجرائم المنصوص عليها في صلب الاتفاقية دون وجه حق.
- أن ترتكب الجرائم المنصوص عليها في الاتفاقية بطريقة عمدية، من أجل إقرار المسؤولية الجنائية.

الفرع الثاني: القانون العربي النموذجي الاسترشادي لمكافحة الجريمة المعلوماتية:

يعد القانون العربي النموذجي لمكافحة جرائم الكمبيوتر، خطوة فعالة في مجال مكافحة الجريمة المعلوماتية، ومسلك منطقي وضروري لابد من اتخاذه، لأن المجتمعات العربية ليست بمنأى عن هذه الجرائم الجديدة، كما أن ارتباط الدول ببعضها البعض في شتى مجالات الحياة بفضل التطور المعلوماتي الذي وصل إليه العالم اليوم يفرض ضرورة التعامل المثلي، في مواجهة

---

[1] - محمد السعيد زناتي، المرجع السابق، ص، 37.

[2] - دري فيصل، المرجع السابق، ص. 29.

[3] - محمد علي العريان، المرجع السابق، ص. 26.

الجريمة بصفة عامة والجريمة المعلوماتية بصفة خاصة، نظرا لخصوصيتها وميزاتها التي من أهمها كونها جريمة متعدية الحدود[1].

وقد اعتمد مجلس وزراء العدل العرب، قانون الإمارات العربي لمكافحة جرائم تقنية المعلومات وما في حكمها لسنة 2004، في دورته التاسعة عشرة، والذي جاء متكون من 27 مادة[2].

وأعقبه بعد ذلك مجلس وزراء الداخلية العرب في الدورة الحادية والعشرون، ثم بعد ذلك طلب من الأمانة العامة التابعة لجامعة الدول العربية تعميمه، على وزارات الداخلية للدول العربية الأعضاء للاستفادة منه. وبالرغم من وجاهة القانون، إلا أن معظم الدول العربية، لم تواكبه بتشريعات داخلية تفعل القانون[3].

ومن الجرائم المعلوماتية التي نص عليها القانون العربي النموذجي، نجد جريمة غسل الأموال عبر الوسائط الالكترونية، التي نصت عليها المادة التاسع عشر منه بأنه كل من قام بتحويل الأموال غير المشروعة أو نقلها أو تمويه للمصدر غير المشروع لها أو إخفائه أو قام باستخدام او اكتساب أو حيازة للأموال، مع العلم بأنها مستمدة من مصدر غير مشروع، عن طريق استخدام الحاسب الالكتروني، أو شبكة المعلومات الدولية بقصد إضفاء الصفة المشروعة على تلك الأموال، وتترك العقوبة وفقا لتقدير كل دولة[4].

إضافة إلى جريمة التزوير المعلوماتي التي نصت عليها المادة الرابعة من القانون النموذجي[5]، وجريمة اختراق النظم المعلوماتية التي نصت عليها المادة الثالثة منه[6]، وجريمة السرقة المعلوماتية التي نصت عليها المادة الرابعة عشر على سرقة المعلومات بتجريم كل من عمليات نسخ ونشر المصنفات الفكرية أو الأدبية، أو الأبحاث العلمية أو ما في حكمها، إذا ما ارتكبت دون

---

[1] - دري فيصل، المرجع السابق، ص. 33.

[2] - قرار مجلس وزراء العدل العرب في الدورة التاسعة عشر، الرقم 495-د19-2003/10/8

[3] - نوفل علي عبد الله الصفو، جريمة إنشاء موقع أو نشر معلومات مخلة بالآداب العامة بوسائل تقنية المعلومات (دراسة مقارنة)، المجلة المصرية للدراسات القانونية والاقتصادية ، عدد 3، يناير 2005، ص. 37.

[4] - بدري فيصل، المرجع السابقن ص. 35.

[5] - بنص المادة الرابعة :" كل من زور المستندات المعالجة آليا أو البيانات المخزنة في ذاكرة الحاسوب أو على شريط أو أسطوانة مضغوطة أو غيرها من الوسائط يعاقب وتترك العقوبة وفقا لتقدير الدولة."

[6] - تنص المادة الثالثة من القانون النموذجي العربي: " كل من توصل بطريقة التحايل لاختراق نظم المعالجة الآلية للبيانات يعاقب بالحبس الغرامة و تترك العقوبة لتقدير الدولة."

وجه حق، بعقوبة الحبس التي يترك تقديرها وفقا لقانون كل دولة ودون الاخلال بالنصوص الخاصة بالملكية الفكرية لكل بلد[1].

الفرع الثالث: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:

جاءت هذه الاتفاقية في إطار تعزيز التعاون بين الدول العربية، في مجال مكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحا، وسلامة مجتمعاتها، حيث عقدت هذه الاتفاقية بمدينة القاهرة بجمهورية مصر العربية بتاريخ 21 ديسمبر 2010، في إطار انعقاد مجلسي وزراء الداخلية والعدل العرب المشترك بمقر جامعة الدول العربية بالقاهرة.

حررت هذه الاتفاقية في 43 مادة ضمن خمس فصول، ووقعت عليها الجزائر فور صدورها، وبذلك أصبحت رافدا من روافد التشريع الوطني في إطار مكافحة الاجرام الالكتروني[2].

خاتمة:

أن الانتشار الواسع لهذا النوع من الجرائم، التي واكبت عصر التقدم التكنولوجي خصوصا بعد ظهور شبكة الانترنت، والتي تمتاز بأساليب التكنولوجيا الحديثة والمتطورة، وسرعة وبداهة مرتكبيها، والتي تجعلهم دائما يفلتون من العقاب، في ظل غياب الدليل المادي للجريمة، إضافة إلى غياب منظومة تشريعية دولية صارمة في احكامها وقواعدها لأجل ردعها، باعتبارها هي جريمة عابرة للحدود في وصفها.

فكل هذه الامور تجعل الجريمة الالكترونية موضوع لايزال يكتنزه اللبس والغموض، فعلى الرغم من سن العديد من الاتفاقيات الدولية والاقليمية التي سبق التطرق لها، إلا أنها تبقى غير كافية في ظل غياب تظافر الجهود الدولية وانشاء مرصد لهذا النوع من الجرائم وقضاء متخصص لأجل ردعها، إضافة إلى ضرورة تعاون الدول في مجال مكافحتها، وتسليم المجرمين.

1 - بدري فيصل، المرجع السابق، ص. 38.

2 - محمد السعيد زناتي، المرجع السابق، ص. 38.



منشورات

المركز الديمقراطي العربي

للدراسات الاستراتيجية والاقتصادية والسياسية

برلين – ألمانيا

Berlin10315 Gensingerstr :112

Tel :0049-code Germany

54884375-030

91499898-030

86450098-030

book@democratica.de